House of Lords
House of Commons

Joint Committee on the Draft Investigatory Powers Bill

Draft Investigatory Powers Bill

Report

EMBARGOED until 09:30 on 11 February 2016

HL Paper 93
HC 651

EMBARGOED until 09:30 on 11 February 2016

House of Lords
House of Commons

Joint Committee on the Draft Investigatory Powers Bill

Draft Investigatory Powers Bill

Report

Report, together with formal minutes relating to the report

Ordered by the House of Lords to be printed on 3 February 2016
Ordered by the House of Commons to be printed on 3 February 2016

EMBARGOED until 09:30 on 11 February 2016

HL Paper 93
HC 651
Published on 11 February 2016
by authority of the House of Lords and House of Commons
London: The Stationery Office Limited
£0.00

The Joint Committee on the Draft Investigatory Powers Bill

The Joint Committee on the Draft Investigatory Powers Bill was appointed by the House of Commons on 5 November 2015 and the House of Lords on 25 November 2015 to examine the Draft Investigatory Powers Bill and to report to both Houses by 11 February 2016. The Committee ceased to exist on its production of this Report.

Membership

HOUSE OF LORDS

The Rt Hon Lord Murphy of Torfaen (Labour, Chairman)
Baroness Browning (Conservative)
The Rt Hon Lord Butler of Brockwell (Crossbench)
The Rt Rev Lord Bishop of Chester (Bishops)
Lord Hart of Chilton (Labour)
The Rt Hon Lord Henley (Conservative)
Lord Strasburger (Liberal Democrat)

HOUSE OF COMMONS

Victoria Atkins MP (Conservative)
Suella Fernandes MP (Conservative)
The Rt Hon David Hanson MP (Labour)
Shabana Mahmood MP (Labour)
Stuart C McDonald MP (Scottish National Party)
Dr Andrew Murrison MP (Conservative)
Matt Warman MP (Conservative)

Powers

The Committee had the power to send for persons, papers and records; to sit notwithstanding any adjournment of the House; to report from time to time; to appoint specialist advisers; and to adjourn from place to place within the United Kingdom.

Publication

The Report of the Committee was published by The Stationery Office by Order of both Houses. All publications of the Committee (including press notices) are on the Internet at http://www.parliament.uk/draft-investigatory-powers

Committee staff

The staff of the Committee were Duncan Sagar (Lords Clerk), Liam Laurence Smyth (Commons Clerk), Donna Davidson (Second Lords Clerk), Matt Korris (Policy Analyst), Hannah Stewart (Legal Specialist), Claire Morley (Legal Specialist), Joseph Coley (Lords Committee Assistant), Ian Hook (Commons Committee Assistant) and Clare Ramsaran (Press Officer).

Contacts

All correspondence should be addressed to the Clerk of the Joint Committee on the Draft Investigatory Powers Bill, House of Lords, Millbank House, London, SW1A 0PW. The telephone number for general enquiries is 020 7219 8443; the Committee's email address is draftinvestigatorypowersbill@parliament.uk.

EMBARGOED until 09:30 on 11 February 2016

Contents

Summary 5

Conclusions and recommendations 7

1 Introduction 25

Our inquiry 25

The purpose of pre-legislative scrutiny 25

The timescale for this inquiry 25

The structure of this report 26

2 Legal and policy context of the draft Bill 27

Overview 27

The current legislative framework 27

The Draft Communications Data Bill 27

European law and the Data Retention and Investigatory Powers Act 2014 28

Human Rights Act 1998 29

Recent Reviews of Investigatory Powers in the UK 30

Publication of the draft Bill 31

Concurrent parliamentary inquiries 32

What's in the draft Bill? 32

3 Capabilities 38

Overview 38

Targeted Interception 38

The case for Targeted Interception 38

Communications Data 39

The background to Communications Data 39

The case for Communications Data 39

The intrusiveness of communications data and privacy risks 41

Definitions of communications data 42

Public bodies who may obtain communications data 46

Purposes for which communications data may be obtained 47

Internet Connection Records 48

The case for ICRs 48

The case against ICRs 49

The definition of ICRs 51

The feasibility of ICRs 54

The purposes for which ICRs can be used 59

EMBARGOED until 09:30 on 11 February 2016

Data Retention 60
Security of retained data and privacy risks 62
Retention period 64
Costs 66
Third party data 68
Definitions of telecommunications provider and telecommunications service 70
Retention notices 72
Request Filter 73
Encryption 76
Equipment interference 79
Overview 79
The case for Equipment Interference 81
The case against Equipment Interference 82
Criticism of Equipment Interference 83
Admissibility of evidence 85
Bulk powers 86
The clarity of bulk powers 87
Legality of bulk powers 89
Effectiveness of bulk powers 90
Safeguards for bulk powers 93
Bulk interception 94
Bulk acquisition of communications data 96
Bulk equipment interference 97
Bulk personal datasets 99
Overview 99
Support for BPDs 100
Opposition to BPDs 100
Lack of information about BPDs 102
Excluded datasets 103
Safeguards required for BPDs 104

4 Authorisation regimes 106

Overview 106
Overarching issues 106
Judicial Authorisation 106
Judicial Review 109
Targeted Interception 112
Modification of warrants 112

EMBARGOED until 09:30 on 11 February 2016

Authorising interception in Scottish psychiatric hospitals 112
Targeted Equipment Interference 113
Differences in authorisation and modification for law enforcement and intelligence agencies 113
Discrepancy between draft Bill and Code of Practice 114
Issues common to targeted interception and targeted equipment interference warrants 115
Urgent Warrants 115
Thematic Warrants 116
Communications Data and Internet Connection Records 117
Authorisation for Targeted Communications Data and ICRs 117
Local Authority authorisation 119
Serious Fraud Office authorisation 119
Emergency authorisation procedures 120
Powers to modify Clause 54 and Schedule 4 120
Bulk powers warrants 121
Necessity and Proportionality test 121
Bulk personal datasets 122
Technical Capability notices and National Security notices 122
Process for issuing these notices 122
Data sharing and Extraterritoriality 123
Safeguards for data sharing overseas 124
Dangers and difficulties of asserting extraterritoriality 125
Privileged communications 127
Legal Professional Privilege 127
Journalistic Privilege 131
Parliamentary Privilege 135

5 Oversight 138

Current oversight regime 138
Commissioners or a Commission? 139
Judicial Commissioners 140
Creation of a single oversight body 141
Appointment 141
Re-appointment and length of terms 143
Dismissal 145
Funding 146
Power to modify the functions of the Judicial Commissioners 148

EMBARGOED until 09:30 on 11 February 2016

Impact of authorisation and oversight functions being exercised by the same body 149
Error-reporting and notification 150
Powers and duties of the Judicial Commissioners 152
Constraint on Judicial Commissioners 152
Whistle blowers and the Judicial Commissioners 153
Legal advice and access 154
Technical advice and access 155
Other powers and duties 155
Issuing guidance 157
The Investigatory Powers Tribunal 157
Power of appeal 157
Review of procedures and processes 159
The oversight landscape 161
Privacy and Civil Liberties Board 161

6 Remaining issues 162
The inadmissibility of intercept material as evidence 162
Disclosure of intercept evidence to judges and prosecutors 162
Power to make consequential provision 163
Non-Technical Definitions 164
National Security 164
Economic well-being 165
Publication of codes of practice 166
Bulk data, automated analysis and the right to privacy 167
A review provision 168

Appendix 1: Members and interests 170

Appendix 2: Call for Evidence 172

Appendix 3: Delegated Powers Memorandum 175

Appendix 4: Human Rights Memorandum 180

Appendix 5: List of abbreviations 181

Formal Minutes 183

Witnesses 189

Published written evidence 191

EMBARGOED until 09:30 on 11 February 2016

Summary

The nature and extent of internet activity have expanded exponentially since the coming into force of the Regulation of Investigatory Powers Act (RIPA) in 2000. This trend has had two contrasting consequences for the heated debates which have surrounded the Draft Investigatory Powers Bill. It is unarguable that citizens' private lives and inner thoughts are now captured in communications technology to a far greater extent than previously. Intrusion by the state into this private sphere must only be done reluctantly and on grounds of necessity. At the same time, the movement of activity online includes criminal and terrorist activity, increasingly taking advantage of freely available technology which is by default encrypted. This second consequence has created new challenges for law enforcement and the security and intelligence agencies.

Resolving the tension between privacy and effective law enforcement in this area is no easy task. The Home Office has now come forward with a draft Bill which seeks to consolidate in a clear and transparent way the law enabling all intrusive capabilities. The Committee, together with the many witnesses who gave evidence to us, was unanimous on the desirability of having a new Bill.

The major change which would be brought about by the draft Bill is the creation of a new judicial oversight body and the much greater involvement of judges in the authorisation of warrants allowing for intrusive activities. As well as being important in in its own terms, making this change will reduce the risk that the UK's surveillance regime is found not to comply with EU law or the European Convention on Human Rights. We make a number of detailed recommendations aimed at ensuring that this new system delivers the increased independence and oversight which have been promised.

A proposal which has attracted much attention from our witnesses is that of the creation of an obligation on communications service providers to collect and retain users' internet connection records (ICRs). We heard a good case from law enforcement and others about the desirability of having such a scheme. We are satisfied that the potential value of ICRs could outweigh the intrusiveness involved in collecting and using them. But we also heard strong concerns, in particular from some of the providers themselves, about the lack of clarity over what form the ICRs would take and about the cost and feasibility of creating and storing them. The Home Office has further work to do before Parliament can be confident that the scheme has been adequately thought through.

Other concerns were over the provisions in the Bill for bulk powers to intercept, to acquire communications data and to interfere with equipment. These powers are not new, but have been avowed for the first time in legislation. The public debate over these powers is a healthy one, and the Home Office should ensure that it and the security and intelligence agencies are willing to make their case strongly in the months ahead.

We make a number of other detailed recommendations, including those aimed at ensuring that vital protections for lawyers and journalists are not compromised.

Much of the important detail about the way the new legislation will work is to be contained in a set of Codes of Practice. We call on the Government to ensure that these Codes are published alongside the Bill to inform the further scrutiny which the Bill

EMBARGOED until 09:30 on 11 February 2016

will receive from the two Houses. In our view, the Bill would also benefit from a post-legislative review by Parliament five years after its enactment. We call for provisions for such a review to be included in the Bill.

EMBARGOED until 09:30 on 11 February 2016

Conclusions and recommendations

Introduction

1. The Committee was hugely appreciative of our witnesses' willingness to submit evidence to a challenging deadline. The quality and range of our written evidence has allowed us to make a serious attempt at scrutinising the draft Bill with the necessary degree of rigour. (Paragraph 6)

2. The Committee is grateful to all those who appeared in person before it, often at necessarily short notice. (Paragraph 7)

Targeted Interception

3. We agree that the targeted interception power should be part of the Bill, subject to appropriate warrant authorisation arrangements. (Paragraph 42)

Communications Data

4. We agree that the power to obtain communications data is an important tool for law enforcement and other public bodies. It should be included in the Bill. (Paragraph 58)

5. We acknowledge the difficulty of providing definitions broad enough to capture the variety of ways in which communications are conducted, and may be conducted in the future, while still providing sufficient clarity and precision. (Paragraph 68)

6. We are grateful that the Government has provided further information on the interpretation of communications data and content. We have not had an opportunity to seek views as to whether the definitions are now sufficiently clear. Parliament will need to look again at this issue when the Bill is introduced. We urge the Government to undertake further consultation with communications service providers, oversight bodies and others to ascertain whether the definitions are sufficiently clear to those who will have to use them. (Recommendation 1) (Paragraph 69)

7. We are concerned about the potential detail that entity data might encompass in relation to telecommunications providers, such as Facebook and Google, who build detailed automated profiles of their users. The Government should say whether it wishes to acquire such data in principle and, if not, how it will ensure that the entity data it requests and receives is not of that level of detail. (Paragraph 73)

8. The definition of data in Clause 195 is unclear, unhelpful and recursive. The Government must provide a meaningful and comprehensible definition of data when the Bill is introduced. (Recommendation 2) (Paragraph 76)

9. We agree that local authorities and trading standards should continue to have access to communications data to support their law enforcement roles, but this intrusive power should not be used for minor infringements. (Paragraph 82)

EMBARGOED until 09.30 on 11 February 2016

10. We recommend that Parliament should give further consideration to defining the purposes for which local authorities may be allowed to apply for communications data when the Bill is introduced. (Recommendation 3) (Paragraph 83)

11. We believe that law enforcement should be able to apply for all types of communications data for the purposes of 'saving life'. We recommend that the Home Office should undertake further consultation with law enforcement to determine whether it is necessary to amend Clause 46 (7)(g) to make this explicit on the face of the Bill. (Recommendation 4) (Paragraph 87)

Internet Connection Records

12. We consider that, on balance, there is a case for Internet Connection Records as an important tool for law enforcement. We have concerns about the definitions and feasibility of the existing proposal, which the Home Office must address. These are set out in the following sections. It is also important for ICRs to be properly authorised and overseen, and these issues will be considered in subsequent chapters. (Paragraph 106)

13. We recommend that the Government should publish in a Code of Practice alongside the Bill advice on how data controllers should seek to minimise the privacy risks of subject access requests for ICRs under the Data Protection Act 1998. (Recommendation 5) (Paragraph 107)

14. While we recognise that ICRs could prove a desirable tool for law enforcement agencies, the Government must address the significant concerns outlined by our witnesses if their inclusion within the Bill is to command the necessary support. (Recommendation 6) (Paragraph 108)

15. We acknowledge that, as with communications data, it is difficult to provide definitions of ICRs broad enough to capture the variety of ways in which communications are conducted on the internet, and may be conducted in the future, while still providing sufficient clarity, technical detail and precision. (Paragraph 120)

16. We welcome the additional information the Home Office has provided on ICRs, though we are not in a position to assess the extent to which it meets the concerns of witnesses as to a lack of clarity. (Paragraph 121)

17. We recommend that the definition of Internet Connection Records should be made consistent throughout the Bill and that the Government should give consideration to defining terms such as 'internet service' and 'internet communications service'. We recommend that more effort should be made to reflect not only the policy aims but also the practical realities of how the internet works on a technical level. (Recommendation 7) (Paragraph 122)

18. We do not believe that ICRs are the equivalent of an itemised telephone bill. However well-intentioned, this comparison is not a helpful one. (Paragraph 126)

19. The Committee acknowledges that there are important differences between the ICR proposal in the draft Bill and the system which was used in Denmark. We believe

EMBARGOED until 09:30 on 11 February 2016

that the Home Office has learned lessons from the Danish model that will increase the chances of ICRs being effective. (Paragraph 146)

20. We recommend that the Government should publish a full assessment of the differences between the ICR proposal and the Danish system alongside the Bill. (Recommendation 8) (Paragraph 147)

21. The Committee is grateful to the many witnesses who submitted detailed consideration of Internet Connection Records. We urge the Government to explain in its response to this report how the issues which have been raised about the technical feasibility of ICRs will be addressed in practice. (Paragraph 150)

22. We agree that all of the proposed purposes for which access to ICRs could be sought are appropriate. Furthermore, we recommend that the purposes for which law enforcement may seek to access ICRs should be expanded to include information about websites that have been accessed that are not related to communications services nor contain illegal material, provided that this is necessary and proportionate for a specific investigation. (Paragraph 155)

23. We recommend that the purposes for which law enforcement may seek to access ICRs should be expanded to include information about websites that have been accessed that are not related to communications services nor contain illegal material, provided that this is necessary and proportionate for a specific investigation. (Recommendation 9) (Paragraph 155)

Data Retention

24. While judgements from the European Court of Justice are outstanding, legislation in this area will remain subject to potential change. Whether ICRs are included or not, we believe that, in light of the ongoing need for communications data and the imminent expiry of DRIPA, a continued policy of some form of data retention is appropriate and that these provisions should accordingly form part of the Bill. (Paragraph 162)

25. The security of retained data, especially such potentially intrusive data, is of great importance. We have received assurances from the Home Office that it is possible to hold such data securely if high standards are set, observed, and regularly scrutinised but data theft remains an ongoing challenge. (Paragraph 174)

26. We urge the Government to consider the suggestion to work with the Information Commissioner's Office, the National Technical Assistance Centre and the Communications-Electronics Security Group at GHCQ, which has recognised expertise in this area, to draw up a set of standards for CSPs. (Recommendation 10) (Paragraph 175)

27. We are not convinced that targeted retention orders are a viable alternative to a data retention provision, as they do not provide retrospective information and would be of limited value in instances where criminal action had ceased. (Paragraph 183)

EMBARGOED until 09:30 on 11 February 2016

28. Any fixed retention period will always risk being arbitrary. We believe on balance that law enforcement have made the case for a 12 month retention period and support its inclusion in the Bill. (Paragraph 186)

29. We are not able to make an assessment of the accuracy of the data retention costs provided by the Government. We urge the Government to continue working with CSPs to improve the detail of the cost estimates for data retention to show how it will be deliverable in practice and deliver value for money. (Paragraph 195)

30. As the communications data will be held for purposes that are not related to the CSP's own business purposes, we agree that the Government should provide CSPs with whatever technical and financial support is necessary to safeguard the security of the retained data. While we do not agree that 100% cost recovery should be on the face of the Bill, we do recommend that CSPs should be able to appeal to the Technical Advisory Board on the issue of reasonable costs. (Recommendation 11) (Paragraph 196)

31. Our view is that the Government should provide statutory guidance on the cost recovery models, and that particular consideration should be given to how the Government will support smaller providers served with data retention notices. (Recommendation 12) (Paragraph 197)

32. We agree with the Government's intention not to require CSPs to retain third party data. The Bill should be amended to make that clear, either by defining or removing the term "relevant communications data". (Recommendation 13) (Paragraph 205)

33. We recommend that the Government should clarify the types of data it expects CSPs to generate and in what quantities so that this information can be considered when the Bill is introduced. (Recommendation 14) (Paragraph 209)

34. We believe that the definition of telecommunications service providers cannot explicitly rule out smaller providers without significantly compromising the data retention proposals as a whole. We acknowledge that the potential burden of data retention notices, particularly for smaller providers, could be acute. This makes the clarification of cost models, as we have recommended above, essential. (Paragraph 220)

35. We are reassured that a route of appeal for data retention notices exists in Clause 73. (Paragraph 221)

36. We understand the Government's position for not allowing the fact that a data retention notice has been served to be referred to in public. We suggest that some forum or mechanism, perhaps through the Technical Advisory Board, is made available so that CSPs subject to such notices can share views on how best to comply with them. (Recommendation 15) (Paragraph 228)

37. We believe that the Intelligence and Security Committee and the Investigatory Powers Commissioner should have access to a list of CSPs served with data retention notices and that their scrutiny will be a valuable check on the appropriate use of this power. We also acknowledge that the Information Commissioner's Office will scrutinise the information security arrangements of CSPs subject to data retention

EMBARGOED until 09:30 on 11 February 2016

notices and will therefore need to be informed of the existence and content of relevant notices. (Paragraph 229)

Request Filter

38. We welcome the amendments that have been made to the Request Filter proposal. They constitute an improvement on that which was included in the Draft Communications Data Bill. (Paragraph 238)

39. We welcome the Government's proposal to build and operate a Request Filter to reduce the amount of potentially intrusive data that is made available to applicants. We believe that the technical and security challenges involved in implementing the Request Filter can be met and would urge the Investigatory Powers Commissioner to examine and report on it to ensure that it is secure. (Paragraph 246)

40. We acknowledge the privacy risks inherent in any system which facilitates access to large amounts of data in this manner. We believe that the requirement upon law enforcement to state the operational purpose for accessing data through the filter will provide an important safeguard that can be assessed by the Investigatory Powers Commissioner and that the oversight of the Commissioner will be sufficient to prevent the Request Filter being used for "fishing expeditions" and ensure that it is used proportionately. (Paragraph 247)

Encryption

41. We agree with the intention of the Government's policy to seek access to protected communications and data when required by a warrant, while not requiring encryption keys to be compromised or backdoors installed on to systems. The drafting of the Bill should be amended to make this clear. (Recommendation 16) (Paragraph 263)

42. The Government still needs to make explicit on the face of the Bill that CSPs offering end-to-end encrypted communication or other un-decryptable communication services will not be expected to provide decrypted copies of those communications if it is not practicable for them to do so. We recommend that a draft Code of Practice should be published alongside the Bill for Parliament to consider. (Recommendation 17) (Paragraph 264)

Targeted Equipment Interference

43. The Committee welcomes the fact that the EI techniques and powers are now properly addressed in legislation. (Paragraph 268)

44. We are grateful for the information provided about EI on visits to the Metropolitan Police and to GCHQ, which has assisted our ability to scrutinise this power. (Paragraph 272)

45. We agree that targeted equipment interference has the potential to be very intrusive. (Paragraph 286)

EMBARGOED until 09:30 on 11 February 2016

46. There is nevertheless a substantive case for the targeted equipment interference power. We believe that, subject to the appropriate authorisation process involving a Judicial Commissioner, such activities should be conducted when necessary and proportionate. (Paragraph 287)

47. We recommend that the Government should produce a Code of Practice on Equipment Interference to cover the activities both of the security and intelligence agencies and of law enforcement. (Recommendation 18) (Paragraph 288)

48. We note that, if our recommendation for post-legislative review five years after the Bill's enactment is implemented, a tighter definition can be introduced without running the risk of law enforcement and the agencies being left behind by technological advancement. (Paragraph 292)

49. We acknowledge both the concerns of witnesses about the breadth of the definitions and the desire of Government not to inadvertently rule out access to new types of equipment or system in the future. (Paragraph 293)

50. We believe that the involvement of Judicial Commissioners in the authorisation process may ensure that the equipment and systems targeted by EI activities will be proportionate and considered foreseeable. (Paragraph 294)

51. We recommend that the Government should produce more specific definitions of key terms in relation to EI to ensure greater confidence in the proportionality of such activities and that a revised Code of Practice is made available alongside the Bill. (Recommendation 19) (Paragraph 295)

52. We acknowledge the importance of data protection in relation to EI activities. We recommend that the assessments undertaken by Judicial Commissioners when authorising warrants should give consideration to data protection issues. (Recommendation 20) (Paragraph 298)

53. We further recommend that the Home Office should make clear in the explanatory notes to the Bill or in a Code of Practice how EI activities can be conducted within the constraints of data protection legislation. (Recommendation 21) (Paragraph 299)

54. We agree that material acquired through targeted equipment interference warrants should be admissible in court, though we share the concerns of witnesses about the risks involved. We believe that law enforcement and the security and intelligence agencies will need detailed codes of practice and appropriate procedures to ensure that evidence is not inadvertently compromised. We urge the Government to consider how it will reconcile the understandable desire of law enforcement and the security and intelligence agencies to keep their techniques secret with the need for evidential use and disclosure regimes in legal proceedings. (Recommendation 22) (Paragraph 305)

Bulk Capabilities

55. We commend the Home Office for making explicit provision for these bulk powers and for giving the Parliament an opportunity to debate and decide upon them. (Paragraph 309)

EMBARGOED until 09.30 on 11 February 2016

56. We recommend that the Government should publish a fuller justification for each of the bulk powers alongside the Bill. We further recommend that the examples of the value of the bulk powers provided should be assessed by an independent body, such as the Intelligence and Security Committee or the Interception of Communications Commissioner. (Recommendation 23) (Paragraph 319)

57. We recognise that, given the global nature of the internet, the limitation of the bulk powers to "overseas-related" communications may make little difference in practice to the data that could be gathered under these powers. We recommend that the Government should explain the value of including this language in the Bill. (Recommendation 24) (Paragraph 323)

58. It is possible that the bulk interception and equipment interference powers contained in the draft Bill could be exercised in a way that does not comply with the requirements of Article 8 as defined by the Strasbourg court. It will be incumbent upon the Secretary of State and judicial commissioners authorising warrants, and the Investigatory Powers Commissioner's oversight of such warrants, to ensure that their usage is compliant with Article 8. (Paragraph 331)

59. We are aware that the bulk powers are not a substitute for targeted intelligence, but believe that they are an additional resource. Furthermore, we believe that the security and intelligence agencies would not seek these powers if they did not believe they would be effective and that the fact that they have been operating for some time would give them the confidence to assess their merits. (Paragraph 340)

60. National security considerations mean that we are not well-placed to make a thorough assessment of the value of the bulk powers. The scrutiny and conclusions of the Intelligence and Security Committee on the Bill will be of significant assistance for Parliamentarians considering these powers. (Paragraph 341)

61. We are grateful to the Home Secretary for the additional information she provided on safeguards for bulk powers, but note that her letter arrived too late for other witnesses to give the Committee their views upon it. (Paragraph 347)

62. In general, we are content that the safeguards proposed by the Home Office, buttressed by authorisation by Judicial Commissioners and oversight from the Investigatory Powers Commissioner will be sufficient to ensure that the bulk powers are used proportionately. (Paragraph 348)

63. We acknowledge, though, the call for greater safeguards for the bulk powers. We believe that it is difficult to make a thorough assessment of the effectiveness of further safeguards without a greater understanding of the way in which bulk powers are operated in practice. (Paragraph 349)

64. We recommend that the Investigatory Powers Commissioner, within two years of appointment, should produce a report to Parliament considering the safeguards that exist and making recommendations for improvements if required. (Recommendation 25) (Paragraph 349)

65. We agree that bulk communications data has the potential to be very intrusive. As with the other bulk powers, we believe that the fuller justification which we have

EMBARGOED until 09:30 on 11 February 2016

recommended the Government produces and the conclusions of the Intelligence and Security Committee on the Bill will assist Parliament's consideration of the necessity and appropriateness of bulk acquisition. (Paragraph 362)

66. We recommend that applications for targeted and bulk EI warrants should include a detailed risk analysis of the possibilities of system damage and collateral intrusion and how such risks will be minimised. We also recommend that such warrants should detail how any damaged equipment will be returned to its previous state at the point that the authorisation or operational need ceases. (Recommendation 26) (Paragraph 372)

67. We acknowledge the concerns of CSPs and other companies who may be required to be complicit in EI activities. We believe that, on balance, it is necessary, subject to a warrant that has been authorised as necessary and proportionate by the Secretary of State and a Judicial Commissioner. (Paragraph 373)

68. We recommend that the Code of Practice on equipment interference should set out how individuals and companies should be engaged with when conducting authorised EI activities to make the process more transparent and foreseeable. (Recommendation 27) (Paragraph 374)

Bulk Personal Datasets

69. We are grateful to the Home Secretary for the additional information she provided to the Committee on bulk personal datasets (BPDs). We believe that that the lack of a formal case for BPDs remains a shortcoming when considering the appropriateness of this power. (Paragraph 389)

70. We recommend that the Home Office should produce its case for bulk personal datasets (BPDs) when the Bill is published. (Recommendation 28) (Paragraph 390)

71. We recommend that the Intelligence and Security Committee, in their analysis of BPDs, should assess the extent to which the concerns expressed by witnesses are justified. (Recommendation 29) (Paragraph 391)

72. While the Committee acknowledges the case made by the Home Office for not providing detailed information as to the contents of bulk personal datasets (BPDs), the lack of that detail makes it hard for Parliament to give the power sufficient scrutiny. (Paragraph 403)

73. The safeguards for BPDs are not sufficiently explained in the Bill. We have not seen a draft Code of Practice on BPDs, and we therefore do not know whether BPDs will, in practice, be treated differently from the communications datasets that are referred to in parts 4 and 6 of the Bill (and which also appear to fall under the definition of a BPD). (Paragraph 406)

74. We believe that a draft Code of Practice on BPDs should be published when the Bill is introduced to provide greater clarity on the handling of BPDs, not least in relation to the provisions of the Data Protection Act 1998. To the greatest extent possible, the safeguards that appear in the Data Protection Act 1988 should also apply to

EMBARGOED until 09:30 on 11 February 2016

personal data held by the security and intelligence agencies. (Recommendation 30) (Paragraph 407)

75. We also agree that existing powers for acquiring BPDs should be consolidated in this Bill and that any other powers for the security and intelligence agencies to acquire BPDs should be repealed. (Recommendation 31) (Paragraph 408)

Authorisation of Warrants

76. The Committee is satisfied that a case has been made for having a 'double-lock' authorisation for targeted interception, targeted equipment interference, and bulk warrants. (Paragraph 421)

77. The Committee is satisfied with the wording in the Bill and believes that the judicial review principles will afford the Judicial Commissioners a degree of flexibility, as outlined by the Home Secretary. (Paragraph 433)

Authorisation of Targeted Interception

78. The Committee believes that a modification, as currently worded in the draft Bill, might include adding a whole new set of people or premises to an existing warrant. The warrant could therefore be changed in a substantial way without any judicial oversight. (Paragraph 438)

79. The Committee recommends that major modifications for targeted interception warrants, as defined in the draft Bill, should also be authorised by a Judicial Commissioner. (Recommendation 32) (Paragraph 439)

80. The omission of a reference to the Mental Health (Care and Treatment) (Scotland) Act appears to us to be an oversight, which we agree could lead to the creation of conflicting authorisation regimes for the use of interception in psychiatric hospitals in Scotland. (Paragraph 443)

81. The Committee recommends that this apparent oversight be addressed in the revised Bill. (Recommendation 33) (Paragraph 443)

82. We recommend that the Home Office should further review its list of investigatory powers in other legislation to ensure that nothing else has been overlooked. (Recommendation 34) (Paragraph 444)

Authorisation of Targeted Equipment Interference

83. The Committee believes that the differential approach to authorisations and modifications for targeted equipment interference warrants applied to the security and intelligence agencies and law enforcement agencies is confusing and unjustified. (Paragraph 450)

84. We therefore recommend that the approach to targeted equipment interference warrants should be standardised and that all modifications should be subject to judicial authorisation. (Recommendation 35) (Paragraph 450)

EMBARGOED until 09.30 on 11 February 2016

85. The Committee is satisfied that the safeguards for equipment interference are adequately set out in the Code of Practice and do not need to also be reflected on the face of the Bill. (Paragraph 452)

Authorisation of Urgent Warrants

86. While the Committee accepts that there will be some exceptionally urgent circumstances in which a warrant will need to be authorised immediately, it is not clear why the period for the Judicial Commissioner to review and authorise the warrant should be as long as five working days. (Paragraph 456)

87. The Committee therefore recommends that the period in which urgent warrants must be reviewed by a Judicial Commissioner should be shortened significantly. We suggest that they must be reviewed within 24 hours of their signature by the Secretary of State (Recommendation 36) (Paragraph 457)

88. We agree that greater clarity on the term "urgent" is required. (Paragraph 458)

89. The Committee recommends the inclusion of a definition of the word "urgent" for the purposes of authorising urgent warrants. (Recommendation 37) (Paragraph 460)

Authorisation of Thematic Warrants

90. The Committee agrees that the current wording of the provisions for targeted interception and targeted equipment interference warrants is too broad. (Paragraph 467)

91. The Committee recommends that the language of the Bill be amended so that targeted interception and targeted equipment interference warrants cannot be used as a way to issue thematic warrants concerning a very large number of people. (Recommendation 38) (Paragraph 468)

Authorisation of Communications Data

92. The Committee is satisfied that the proposed authorisation process for communications data is appropriate but recommends that extra protections for privileged and confidential communications should be applied in the same way as is proposed for journalists in Clause 61. (Recommendation 39) (Paragraph 474)

93. The Committee understands the value of local authorities being able to access communications data in limited circumstances and is content with the proposed authorisation process. (Paragraph 478)

94. The Committee recommends the removal of emergency procedures for communications data so that the Single Point of Contact process can never be bypassed. (Recommendation 40) (Paragraph 482)

95. The Committee agrees with the conclusions of the Delegated Powers and Regulatory Reform Committee (DPRRC) on the enhanced affirmative procedure

EMBARGOED until 09.30 on 11 February 2016

for amendments to Clause 54 and Schedule 4. We join them in welcoming the strengthening of scrutiny procedures in this area of the draft Bill. (Paragraph 485)

96. The Committee agrees with the recommendation of the DPRRC on modifications to the list of ranks and offices which must be held by a designated senior officer. We recommend that Clause 56(1) and Clause 57(4) should be amended accordingly. (Recommendation 41) (Paragraph 489)

Authorisation of Bulk Powers

97. Subject to the views of the Intelligence and Security Committee regarding bulk powers, we are confident that the Judicial Commissioners would be able to assess the necessity and proportionality criteria in relation to bulk warrants. (Paragraph 493)

Authorisation of Bulk Personal Datasets

98. The Committee recommends that authorisations for bulk personal datasets should be required to be specific and provisions for class authorisations should be removed from the Bill. The provision relating to replacement datasets (Clause 154(6)) should also be removed. (Recommendation 42) (Paragraph 497)

National Security and Technical Capability Notices

99. The Committee accepts that National Security and Technical Capability notices are different in scope and intrusion to the types of warrants that will need to be authorised by a Judicial Commissioner. We are therefore content that these notices should be issued by the Secretary of State without reference to a Judicial Commissioner. (Paragraph 502)

Intelligence Sharing

100. The Committee believes that leaving the decision regarding the propriety of sharing intercept material with an overseas authority to the appropriate issuing authority is not a strong enough safeguard (Paragraph 510)

101. The Committee would like to see more safeguards for the sharing of intelligence with overseas agencies on the face of the Bill. These should address concerns about potential human rights violations in other countries that information can be shared with. (Recommendation 43) (Paragraph 511)

102. The Committee also recommends that the Bill should make it illegal for UK bodies to ask overseas agencies to undertake intrusion which they have not been authorised to undertake themselves. (Recommendation 44) (Paragraph 512)

Extraterritoriality

103. We recommend that the Government should give more careful consideration to the consequences of enforcing extraterritoriality. The Government should re-double

EMBARGOED until 09:30 on 4 February 2016

its efforts to implement Sir Nigel Sheinwald's recommendations. (Recommendation 45) (Paragraph 518)

Privileged Communications

104. The Committee is concerned that the Bill as drafted only provides (through a proposed code of practice relating to Part 3 of the Bill) for the application of LPP in the case of communications data (despite the information provided by the Home Office which suggests provisions of the code will relate to acquisition of other material). (Paragraph 534)

105. The Committee is further concerned that there are no substantive provisions addressing LPP even in the case of communications data on the face of the Bill and considers that this may call into question the application of LPP when the Bill's powers are exercised, particularly given the judgment in *McE* and the inclusion of specific provisions in other legislation conferring investigatory powers. Additionally, the lack of a draft code prevents the Committee scrutinising provisions on an important matter. (Paragraph 535)

106. The Committee notes the Home Office's concerns about potential abuse of privileges by either lawyers or their clients. (Paragraph 536)

107. The Committee recommends that provision for the protection of Legal Professional Privilege (LPP) in relation to all categories of acquisition and interference addressed in the Bill should be included on the face of the Bill and not solely in a code of practice. The Government should consult with the Law Societies and others as regards how best this can be achieved. (Recommendation 46) (Paragraph 537)

108. The Home Office should review its proposals in relation to LPP to ensure that they meet the requirements of Article 8 and relevant case law. (Recommendation 47) (Paragraph 538)

109. The Committee considers that protection for journalistic privilege should be fully addressed by way of substantive provisions on the face of the Bill. (Paragraph 553)

110. The Committee recommends that the Home Office should reconsider the level of protection which the Bill affords to journalistic material and sources. This should be at least equivalent to the protection presently applicable under PACE and the Terrorism Act 2000. (Recommendation 48) (Paragraph 554)

111. The Committee recommends that if Clause 61 remains in its present form the Bill should make it clear that RIPA and Clause 61 do not act so as to enable the investigatory authorities to avoid the application of PACE or the Terrorism Act and the ability they afford to media to know about an application for communications data and make representations as to the proposed acquisition. (Recommendation 49) (Paragraph 555)

112. The Home Office should review Clause 61 to ensure that it meets the requirements of Article 10 ECHR. (Recommendation 50) (Paragraph 556)

EMBARGOED until 00:30 on 11 February 2016

113. The Committee considers that the approach taken in the Bill to surveillance of Parliamentarians strikes an effective balance between the need for Parliamentarians to be able to communicate fully and frankly with their constituents and other relevant third parties and the needs of the security and intelligence agencies and law enforcement agencies. (Paragraph 564)

Judicial Commissioners

114. It is unclear to us why the Home Office chose to create a group of Judicial Commissioners rather than creating an Independent Intelligence and Surveillance Commission as recommended by David Anderson QC, a recommendation endorsed by the knowledgeable and experienced Interception of Communications Commissioner's Office. The benefits of having a senior independent judicial figure in the Investigatory Powers Commissioner would not be lost by putting the IPC at the head of a Commission. The evidence we have heard is that the work of the oversight body will be significantly enhanced by the creation of a Commission with a clear legal mandate. (Paragraph 574)

115. We recommend that such a Commission should become the oversight body in the Bill. (Recommendation 51) (Paragraph 574)

116. The Judicial Commissioners or Commission should have the power to instigate investigations on their or its own initiative. This is vital in order to ensure effective and independent oversight. The current provisions in the draft Bill on the powers of the Judicial Commissioners do not make it clear that they have this power. We recommend that a power to initiate investigations should appear on the face of the Bill. (Recommendation 52) (Paragraph 575)

117. We welcome the creation of the Judicial Commissioners as a single oversight body which will improve transparency, public confidence and effective oversight of the use of the powers contained in the Bill. (Paragraph 579)

118. We do not think that appointment by the Prime Minister would in reality have any impact on the independence of the Investigatory Powers Commissioner and Judicial Commissioners. In modern times, our senior judges have had an unimpeachable record of independence from the executive and we believe any senior judge appointed to these roles would make his or her decisions unaffected by the manner of appointment. (Paragraph 587)

119. We recommend that the Lord Chief Justice should have the power to appoint Judicial Commissioners following consultation with his judicial counterparts in Scotland and Northern Ireland and with the Prime Minister, Scottish Ministers, and the First Minister and deputy First Minister in Northern Ireland. This will ensure public confidence in the independence and impartiality of the Judicial Commissioners. It will also enhance political confidence in them. The Lord Chief Justice will also be able to assess the impact of appointments on the work of the High Court and the Court of Appeal, which must not be impaired by the creation of the Judicial Commissioners. The Judicial Appointments Commission must also be consulted to ensure that the appointments procedure is fair and transparent. (Recommendation 53) (Paragraph 588)

EMBARGOED until 09:30 on 11 February 2016

120. We accept concerns that having renewable terms of appointment could have negative implications for public confidence in the independence of Judicial Commissioners. We conclude that these concerns strengthen the argument for the power of appointment being held by the Lord Chief Justice, rather than the Prime Minister. (Paragraph 592)

121. The Government should reconsider both the length of terms of appointment and whether they should be renewable. Terms need to be long enough for Judicial Commissioners to build expertise but should not be so long that they have a negative impact on a serving judge's career. It may be that three-year terms with an option for renewal is the most workable solution but we recommend that there should be careful reconsideration of these provisions in consultation with the Lord Chief Justice, Judicial Appointments Commission, the current surveillance Commissioners and other interested parties to ensure the benefits and disadvantages of the different approaches have been thoroughly examined. (Recommendation 54) (Paragraph 593)

122. Maintaining public confidence in the Judicial Commissioners may occasionally require that a Commissioner is removed from the role because he or she has behaved in a manner incompatible with what is, in effect, high judicial office. Public confidence also requires that the power to remove from office does not damage the public perception of the Judicial Commissioners' independence from the executive or the freedom of the Judicial Commissioners to make decisions that may be unpopular with the Government. We believe that the broad powers of dismissal contained in the draft Bill significantly impair the independence of the Judicial Commissioners. We therefore recommend that the Judicial Commissioners be subject to the same dismissal and suspension procedures as those applicable to serving senior judges: removal from office following a resolution of both Houses of Parliament and suspension and other disciplinary measures exercised by the Lord Chief Justice and Lord Chancellor. (Recommendation 55) (Paragraph 597)

123. We believe it is inappropriate for the Home Secretary alone to determine the budget of the public body which is monitoring her exercise of surveillance powers. The Government may want to consider a role for Parliament in determining the budget. (Recommendation 56) (Paragraph 604)

124. Clause 177 contains a power for the Home Secretary to modify the functions of the Judicial Commissioners. While we recognise the concerns of some of our witnesses, we believe such a power is appropriate as we have every confidence such a power would only be exercised responsibly by the Secretary of State. (Paragraph 608)

125. While we accept that the Judicial Commissioners must not be perceived as overseeing their own work, we do not think this is an insurmountable problem. We agree with the Home Secretary that the senior judges who will act as Judicial Commissioners will be well aware of the need to separate the authorisation and oversight functions with which they are entrusted. We emphasise that there needs to be a clear delineation of functions within the Judicial Commissioners in order to ensure public confidence in the independence and impartiality in the exercise of the Commissioners' oversight functions. (Paragraph 612)

EMBARGOED until 09:30 on 11 February 2016

126. Clause 171 changes the existing powers of the relevant commissioners to report errors in the use of surveillance powers to the individuals affected by raising the applicable test and requiring the involvement of the Investigatory Powers Tribunal in making the decision. This approach is cumbersome and unnecessary given there are no concerns over the way the current oversight bodies have used their powers of error-reporting. We recommend that the Investigatory Powers Commissioner exercise the error-reporting power alone, without reference to the Investigatory Powers Tribunal. (Recommendation 57) (Paragraph 621)

127. We recommend that the Government should review the error-reporting threshold in light of the points made by witnesses. (Recommendation 58) (Paragraph 622)

128. It should be made clear in the duties laid on the Judicial Commissioners in subclauses 169(5) and (6) that they must comply with those duties in a proportionate manner. The subclauses are drafted in very broad and uncertain terms which have the potential to impact upon the work of Judicial Commissioners in unintended ways. Public confidence in the independence of the Judicial Commissioners requires clarity and transparency in both powers and duties. We recommend that Clauses 169(5) and (6) should be re-drafted to protect the Judicial Commissioners' independence and to ensure the Judicial Commissioners are not constrained from providing effective oversight. (Recommendation 59) (Paragraph 626)

129. We recommend that the Bill should contain an explicit provision for Communication Service Providers and staff in public authorities to refer directly to the Judicial Commissioners any complaint or concern they may have with the use of the powers under the Bill or any request for clarification on the use of those powers. Where clarification is provided the Judicial Commissioners will need to have the power to make that information public should it be appropriate in the circumstances. This will enable better compliance with the provisions of the Bill and will help to reduce costs. (Recommendation 60) (Paragraph 629)

130. We recommend that members of the security and intelligence agencies should be able to contact the Investigatory Powers Commissioner with concerns over the misuse of surveillance powers without being at risk of prosecution for breaching the Official Secrets Act. The Investigatory Powers Commissioner should then have discretion whether to exercise his or her power to initiate an inquiry into the allegations. We recognise that there may be wider concerns over the role of whistle-blowers in this area. This is a matter which requires consultation and therefore this is not the appropriate Bill in which those wider concerns should be taken forward. (Recommendation 61) (Paragraph 630)

131. The law in this area is complex and developing. Judicial Commissioners will have to make decisions without the benefit of adversarial argument. We agree with the Independent Reviewer of Terrorism that Judicial Commissioners must have access to both in-house legal expertise and, on request, security-cleared independent counsel to assist them in both the authorisation and oversight functions of their role. (Recommendation 62) (Paragraph 634)

132. We recommend that the Judicial Commissioners should have a legal mandate to access all relevant technical systems required to ensure effective oversight of the

EMBARGOED until 09:30 on 11 February 2016

powers contained in the Bill. This mandate should appear on the face of the Bill. (Recommendation 63) (Paragraph 637)

133. We recommend that the Judicial Commissioners should have access to technical expertise to assist them in fulfilling their authorisation and oversight functions. (Recommendation 64) (Paragraph 638)

134. The Judicial Commissioners should be able to communicate with the Investigatory Powers Tribunal on a point of law without consulting the Home Secretary. Clause 172(3) should be redrafted to reflect this. (Recommendation 65) (Paragraph 640)

135. The Judicial Commissioners should be able to make a direct reference to the Investigatory Powers Tribunal where they have identified unlawful conduct following an inspection, audit, investigation or complaint. (Recommendation 66) (Paragraph 642)

136. The Investigatory Powers Commissioner's annual report must include information about the impact, results and extent of the use of powers in the Bill so effective public and parliamentary scrutiny of the results of the powers can take place. (Recommendation 67) (Paragraph 646)

137. The Investigatory Powers Commissioner should be able to inform the Intelligence and Security Committee if he or she is unhappy about the use of the Prime Minister's power to redact his annual report. (Recommendation 68) (Paragraph 647)

138. We recommend that the Judicial Commissioners should have the power to develop guidance to public authorities to assist them in applications seeking to use investigatory powers. This will help applicant bodies to formulate focused applications saving time and resources. Where the constraints of national security allow, the guidance should be published in the interests of public transparency and foreseeability. (Recommendation 69) (Paragraph 649)

Investigatory Powers Tribunal

139. We recommend that the right of appeal from the Investigatory Powers Tribunal in Clause 181 should be amended to include cases where there has been an error of law to prevent injustice as a matter of public policy and to satisfy the rule of law. (Recommendation 70) (Paragraph 654)

140. We recommend that rulings in the Investigatory Powers Tribunal should be subject to an interim right of appeal on the grounds of an error of law to save time and costs. (Recommendation 71) (Paragraph 655)

141. We recommend that the appeal route for Scotland and Northern Ireland should appear on the face of the Bill. It is unclear to us why there is not a specified route of appeal in Scotland and Northern Ireland nor what appellants in those parts of the United Kingdom are expected to do before the Home Secretary issues regulations on this issue. (Recommendation 72) (Paragraph 656)

EMBARGOED until 09:30 on 11 February 2016

142. The Home Office should conduct a consultation and review of the powers and procedures of the Investigatory Powers Tribunal with the aim of improving openness, transparency and access to justice. (Recommendation 73) (Paragraph 660)

143. The Investigatory Powers Tribunal should have the power to decide whether its proceedings should be held in public. When making a decision on whether a hearing or part of a hearing should be open or not the Tribunal should apply a public interest test. (Recommendation 74) (Paragraph 663)

144. The Investigatory Powers Tribunal should be able to make a declaration of incompatibility under the Human Rights Act. (Recommendation 75) (Paragraph 666)

The Oversight Landscape

145. We have heard evidence that there is potential for the further simplification of the oversight landscape. This would improve transparency, reduce overlaps and ensure consistency of decision-making which would all contribute to ensuring oversight of the powers contained in the Bill comply with international law standards. We recommend that the Home Office should carry out a review to identify areas in which further simplification of oversight could occur. (Recommendation 76) (Paragraph 670)

146. We call on the Government to outline its plans for the establishment of the Privacy and Civil Liberties Board. (Recommendation 77) (Paragraph 671)

Remaining Issues

147. The Committee recommends that the Government keeps the issue of the inadmissibility of intercept material as evidence under review and takes note of the significant perceived benefits of using such material as evidence. (Recommendation 78) (Paragraph 675)

148. The Committee recommends that the Government should consider the Chief Coroner's proposals and engages further with him to come to a satisfactory agreement about which judges can be included in the list in Schedule 3. (Recommendation 79) (Paragraph 679)

149. We agree with this conclusion of the DPRRC on the power in Clause 201 (2) to make consequential provision and recommend the deletion of powers to amend future enactments. (Recommendation 80) (Paragraph 682)

150. We agree with the DPRRC that the negative procedure for these powers is inappropriate and recommend that any modifications to primary legislation be subject to the super-affirmative resolution procedure. (Recommendation 81) (Paragraph 684)

151. The Committee recommends that the Bill should include a definition of national security in order to provide clarity to the circumstances in which these warrants can be issued. (Recommendation 82) (Paragraph 691)

EMBARGOED until 09:30 on 1st February 2016

152. The Committee recommends that the Bill should include a definition of economic well-being in order to provide clarity to the circumstances in which these warrants can be issued. (Recommendation 83) (Paragraph 696)

153. The Codes of Practice will provide essential further details on how the powers in the draft Bill will be used in practice We recommend that all of them should be published when the Bill itself is introduced to allow both Houses to conduct full scrutiny of their contents. (Recommendation 84) (Paragraph 698)

154. We urge the Investigatory Powers Commissioner to scrutinise the automated analysis of bulk datasets conducted by the security and intelligence agencies to ensure that they are conducted appropriately and proportionately and with regard to privacy and data protection requirements. (Recommendation 85) (Paragraph 703)

155. We note the reservations expressed by the Home Secretary about a sunset provision. But we are of the view that some form of review after five years would be merited. We believe that a review provision of this sort, which would require the next Parliament to revisit the powers which are in the draft Bill, would go some way to provide assurance to those who have expressed concerns over the operational case for some of these powers. The evidence of several years' operation will inform the debate. A provision which asked Parliament to revisit the intrusive powers it gives to the Executive after a period would, in our view, be a healthy way to fulfil the welcome aspirations for greater openness and legitimacy which underpin the draft Bill. (Paragraph 708)

156. We agree with the Information Commissioner and others that the provisions of the Bill would benefit from detailed post-legislative scrutiny after an appropriate period. In our view, the appropriate vehicle to do this would be a specially constituted joint committee of the two Houses. This work should begin within six months of the end of the fifth year after which the Bill is enacted. Although the appointment of such a committee would be a matter for the two Houses, a provision in the Bill would provide a clear mandate and guarantee the timescale for this review. (Paragraph 709)

157. We recommend that a provision should be added to the face of the Bill for post-legislative scrutiny by a committee of the two Houses within six months of the end of the fifth year after the Bill is enacted. (Recommendation 86) (Paragraph 710)

EMBARGOED until 09:30 on 11 February 2016

1 Introduction

Our inquiry

1. The Joint Committee was appointed by the House of Commons on 5 November and the House of Lords on 25 November 2015 to conduct pre-legislative scrutiny of the Government's Draft Investigatory Powers Bill ("the draft Bill").

2. The Committee was an *ad hoc* joint committee of the two Houses and ceased to exist on the making of this report.

The purpose of pre-legislative scrutiny

3. The Committee has sought to give the greatest possible early opportunity for stakeholders and the wider public to comment on the draft Bill. In legislation of particular controversy, where many of the facts underpinning arguments on all sides are subject to robust challenge and disagreement, pre-legislative scrutiny can add particular value. It was not possible at this stage to resolve every issue of controversy associated with the draft Bill. In some areas we have simply reported these disagreements and flagged the issues on which we believe particular attention should be concentrated when the Bill itself is introduced. This report will not be the final word of parliamentarians on the issues addressed in the Bill. The publication of the draft Bill, and this Committee's consideration of it, mark the beginning of a parliamentary debate which will continue in the two Houses in the months ahead. Both Houses will give full scrutiny to the Bill proper, a Bill which we believe will be much improved if the recommendations of this report are accepted.

The timescale for this inquiry

4. The Committee was set a reporting deadline by the two Houses of 11 February 2016. Our timescale was framed by the need to replace the Data Retention and Investigatory Powers Act 2014 (DRIPA) before it expires at the end of 2016. This timescale for our work attracted attention from a number of our witnesses.[1]

5. The Committee responded to these timing issues by conducting an intensive programme of evidence taking. We first met on the morning of 26 November, the day after our appointment, and immediately received informal briefings on the draft Bill from officials and others. We issued our public Call for Written Evidence on the following day, Friday 27 November. Our deadline for submissions was necessarily tight, by close on Monday 21 December.

6. Despite the deadline, we received an impressive response, totalling 148 submissions, running to over 1500 pages of evidence. All of this evidence is published with the report. Our witnesses ranged from individuals with an interest to multinational companies and campaign groups as well as representatives of various regulatory arms, and oversight and law enforcement bodies. **The Committee was hugely appreciative of our witnesses'**

1 See written evidence from Big Brother Watch (IPB007) Dr Paul Bernal (IPB018), Entanet International Ltd (IPB0022), Ms Susan Morgan (IPB0043), Article 19 (IPB0052), Mr Ray Corrigan (IPB0053), Duncan Campbell (IPB0069), Mr Howard Clark (IPB0070), Amnesty International UK (IPB0074), Mark Dziecielewski (IPB0082), William Waites (IPB0089), UN Special Rapporteurs (IPB0102), the Chartered Institute of Library Information Professionals (IPB0104), Access Now et al. (IPB0109), ISPA (IPB0137) and McEvedys Solicitors and Attorneys (IPB0138)

EMBARGOED until 09:30 on 11 February 2016

willingness to submit evidence to a challenging deadline. The quality and range of our written evidence has allowed us to make a serious attempt at scrutinising the draft Bill with the necessary degree of rigour.

7. As well as our written evidence, the Committee heard as much evidence in person as it could within the timeframe, including holding meetings on two days when either one House or the other was not sitting. In total we heard from **59** people in **22** public panels. **The Committee is grateful to all those who appeared in person before it, often at necessarily short notice.**

8. To aid its work, the Joint Committee also conducted two informal visits. On 15 December we visited a Metropolitan Police Intelligence Bureau in Vauxhall, where we received a joint briefing from different arms of law enforcement and saw at first hand the process for applying for and approving requests for communications data. On the same day we met representatives of the security and intelligence agencies. In addition, several members of the Committee travelled to Cheltenham to see GCHQ's operations.

9. We were assisted by two specialist advisers, Martin Hoskins and Professor Peter Sommer, to both of whom the Committee is grateful for their insight and counsel. Their interests, together with those of the members of the Joint Committee, are set out in Appendix 1.

The structure of this report

10. Chapter Two explores the policy background to the draft Bill, and attempts to frame its provisions within the wider debates and developments in the UK and elsewhere. Chapter Three sets out the capabilities, some of which are new and others simply avowed in one place for the first time, which the draft Bill would give to law enforcement, the security and intelligence agencies and others. Chapter Four examines the proposed authorisation arrangements for each of these capabilities, and whether they are appropriate. Chapter Five examines the proposed new framework of oversight for the use of the powers in the draft Bill. Chapter Six considers the remaining issues arising from the draft Bill.

EMBARGOED until 09:30 on 11 February 2016

2 Legal and policy context of the draft Bill

Overview

The current legislative framework

11. Much of the existing framework governing the use of investigatory powers is found in the Regulation of Investigatory Powers Act 2000 ("RIPA"). In addition to RIPA, a number of other pieces of statute apply. These include the Telecommunications Act 1984, the Police and Criminal Evidence Act 1984, the Intelligence Services Act 1994, the Terrorism Act 2000, and the Wireless Telegraphy Act 2006.

12. RIPA does not provide obligations on providers to retain data, only on how such data is acquired and disclosed. Prior to 2001, if service providers retained data which could be accessed under RIPA, it would only be data which they were retaining anyway for their own purposes. In response to the attacks on 11 September 2001 an anti-terrorism law, the Anti-terrorism, Crime and Security Act 2001 (ATCSA) was passed. ATCSA introduced a voluntary code which made it possible for details of every website visited, the transmission of every email and SMS text message sent and every phone call made in the UK to be retained for various periods and made available to authorities on request. This position changed again in 2006 when the mandatory retention of data on communications networks was introduced by the EU Data Retention Directive (Directive 2006/24/EC). The Directive was transposed into UK law by the Data Retention (EC Directive) Regulations 2007 and the Data Retention (EC Directive) Regulations 2009.

The Draft Communications Data Bill

13. In June 2012 the coalition Government published the Draft Communications Data Bill. This draft Bill would have replaced RIPA's provisions on the acquisition of communications data. In addition it would have extended significantly the range of data which service providers were required to store. This data would have included more detailed records of each user's internet browsing activity (websites visited but not pages within websites), details of messages sent on social media, webmail, voice calls over the internet, and gaming, in addition to emails, SMS text messages and phone calls.

14. A number of bodies would have had access to this data, chiefly: the Police, the Serious and Organised Crime Agency, the intelligence agencies and HM Revenue and Customs. Such access would not have been subject to judicial authorisation. Access was only permitted if the data was required to investigate crime, protect national security or for range of other specified purposes. The Government argued that the Bill was necessary in order for the police and intelligence and security agencies to operate effectively in a fast-changing environment of communications technology, in which an increasing proportion of communications took place over the internet.

15. A Joint Committee on the draft Bill was appointed in June and reported in December 2012. The Committee concluded that the powers to order the retention of data contained in the Bill should be significantly narrowed, and new safeguards against abuse introduced,

EMBARGOED until 00:30 on 11 February 2016

before these powers could be workable. It also recommended that there should be much better consultation with industry, technical experts, civil liberties groups, public authorities and law enforcement bodies before a new Bill specifying the types of internet data that should be made available to public authorities for investigative purposes was introduced. The Intelligence and Security Committee also published a report raising similar concerns, including that there had been insufficient consultation with Communications Service Providers (CSPs). In the face of an increasingly contentious debate, the draft Bill did not proceed to a Bill proper being introduced.

16. A further area of debate in the Draft Communications Data Bill was over its proposed extension of the scope of powers for local authorities to make potentially intrusive use of communications data. Unlike its predecessor legislation, the Draft Investigatory Powers Bill does not provide new powers to local authorities. It is also worth noting that the Protection of Freedoms Act 2012 has, in the meantime, introduced a tighter regime for the authorisation of access to communications data by local authorities, requiring the approval of a magistrate.

European law and the Data Retention and Investigatory Powers Act 2014

17. In April 2014 the Court of Justice of the European Union (CJEU) produced a ruling, *Digital Rights Ireland*,[2] which found the Data Retention Directive to be invalid because it infringed privacy and data protection rights guaranteed by the EU Charter of Fundamental Rights. The Data Retention Directive, as implemented by secondary legislation in the UK, provided the existing framework requiring the retention of communications data by service providers. The CJEU's ruling therefore had the effect of removing this framework and compromising the ability of law enforcement agencies to access such data if there was no other legitimate reason for service providers to retain it. In response to the ruling, the Government introduced an expedited Bill, which became the Data Retention and Investigatory Powers Act 2014 (DRIPA).

18. DRIPA was subsequently modified by part 3 of the Counter-Terrorism and Security Act 2015 (CTSA), which gave the Secretary of State the ability to require internet service providers to retain data allowing the authorities to identify the person or device using a particular internet protocol (IP) address at any given time.

19. Section 8 of DRIPA contained a 'sunset clause', repealing the Act at the end of 2016. During the Bill's second reading in the Commons, the period of time, some seventeen months, before the sunset clause took effect was criticised by a number of MPs for being longer than was necessary. In response to this, the Home Secretary explained that the period was necessary to allow for subsequent review, including for a Committee such as this one:

> "the reason it has been put at the end of 2016 is that we will have a review by David Anderson which will report before the general election. It is the intention that a Joint Committee of Parliament will look at his work and that of the Intelligence and Security Committee. It will then be necessary to put the required legislation in place. If anyone stops to think about that timetable, it is clear that it could not be completed by the end of this year."[3]

2 European Court of Justice, *Digital Rights Ireland,* C-293/12
3 HC Deb, 15 July 2014, col 714

EMBARGOED until 09.30 on 11 February 2016

20. Section 8 of DRIPA therefore set the terms of the subsequent necessary steps on the path to the introduction of new legislation, at least to provide for data retention.

21. DRIPA has recently been challenged in the UK courts. In November 2015, the Court of Appeal made a reference to the CJEU asking whether the judgment in *Digital Rights Ireland* was intended to lay down mandatory requirements for national legislation that was introduced to comply with European law in this area. The Court of Appeal also asked the CJEU whether *Digital Rights Ireland* was intended to extend data rights protection under European law beyond that available under the right to privacy (Article 8) in the European Convention on Human Rights.[4] We understand that the CJEU is likely to consider this issue before the Bill completes its passage through both Houses.

Human Rights Act 1998

22. The Human Rights Act 1998 incorporates the European Convention on Human Rights (ECHR) into UK law. This means that the draft Bill must comply with the Convention, as must all UK legislation. Article 8 of the ECHR which protects private and family life is of particular relevance in assessing the legality of surveillance and investigatory powers. Article 8(2) requires that any State interference with an individual's right to privacy is both necessary for the furtherance of a legitimate aim such as national security or the prevention and detection of crime, and proportionate. The Home Office view is that the provisions in the draft Bill comply with the Act and resolve "the inevitable tension" between intrusive capabilities and individual rights.[5]

23. The UK's Investigatory Powers Tribunal is currently considering cases brought by Privacy International and others relating to the lawfulness of equipment interference and bulk personal datasets. These legal issues are considered further in the following Chapter, in particular in the context of the data retention and bulk provisions in the draft Bill. In both cases, the Government will have to consider whether it has made appropriate adjustments to reflect existing judgments and to proof the Bill against future judgements of both courts.

24. The UK is not alone in considering how to balance privacy rights against the need to give its law enforcement and intelligence and security agencies the tools to combat crime and terrorism in an increasingly digital world. A number of other EU Member States are in the process of reviewing their national regimes in light of the CJEU's judgment in *Digital Rights Ireland*. Terrorist attacks during the course of 2015 have also prompted some states to seek to provide more intrusive powers for their law enforcement and security and intelligence agencies. Although we did not take enough evidence on international comparisons to draw firm conclusions, comparisons of the degree of judicial involvement in different jurisdictions are worthwhile in considering the proposals for revised authorisation and oversight arrangements in Chapters 4 and 5.

EMBARGOED until 09.30 on 11 February 2016

4 Court of Appeal, *Davis and oths v Secretary of State of the Home Department*, [2015] EWCA Civ 1185
5 Home Office, *Investigatory Powers Bill: European Convention on Human Rights Memorandum*, 4 November 2015

Recent Reviews of Investigatory Powers in the UK

The Anderson Report

25. Section 7 of DRIPA required the Government's independent reviewer of terrorism legislation, David Anderson QC, "to review the operation and regulation of investigatory powers", including "the effectiveness of existing legislation (including its proportionality) and the case for new or amending legislation".

26. David Anderson QC published his report, *A Question of Trust* on 11 June 2015.[6] It was wide-ranging and called for an entirely new legislative framework to replace RIPA and DRIPA. The report also made a series of detailed recommendations, which are considered below as they relate to the provisions of the draft Bill. One of the major recommendations was for the creation of a new body, the Independent Surveillance and Intelligence Commission (ISIC), which would authorise all interception warrants and combine the oversight roles currently filled by three separate commissioners.

The Intelligence and Security Committee

27. The Intelligence and Security Committee of Parliament (ISC) is the body of parliamentarians with which primary oversight of the security and agencies rests. The ISC was established in 1994 under the Intelligence Services Act, and was reformed under the Justice and Security Act 2013. This legislation made the ISC a statutory committee of Parliament and strengthened its powers. The ISC has significantly greater access to information than an investigative select committee such as this joint committee, including access to primary material held within the Agencies. Its remit has also been expanded to include oversight of intelligence and security operations, and oversight of all intelligence and security activities of Government. In the course of its inquiries, the ISC is able to question Ministers and the security and intelligence agencies to hold them to account for their use of intrusive capabilities.

28. In March 2015, the ISC published its report, *Privacy and Security: A modern and transparent legal framework*.[7] The report concluded that the UK's intelligence and security agencies did not seek to circumvent the law but that the legal framework was "unnecessarily complicated" and "lacks transparency". The report called for the consolidation of all current legislation governing the intrusive capabilities of the agencies into a single Act, with all of their capabilities explicitly avowed and the authorisation arrangements for these capabilities set out. The ISC report also paid particular attention to the agencies' use of bulk powers. These powers are explored in the following Chapter of this report. The ISC report rejected calls for a greater degree of judicial involvement in the authorisation of warrants on the grounds that Ministers were "able to take into account the wider context of each warrant application" and were "democratically accountable for their decisions."[8]

EMBARGOED until 09:30 on 11 February 2016

6 David Anderson QC, *A Question of Trust: Report of the Investigatory Powers Review*, 2015

7 Intelligence and Security Committee (ISC), *Privacy and Security: A modern and transparent legal framework*, 12 March 2015, HC 1075

8 *Ibid.*

The Royal United Services Institute

29. In July 2015, the Royal United Services Institute ("RUSI") published its own report, *A Democratic Licence to Operate,* based on the work of an Independent Surveillance Review panel convened at the request of the then Deputy Prime Minister in March 2014.[9] The RUSI report agreed with the ISC and Anderson reports that "the current surveillance powers are needed but that they require a new legislative framework and oversight regime". The report also called for "a composite approach to the authorisation of warrants, dependent on the purpose for which the warrant is sought and subsequent degree of ministerial input required".[10] Warrants relating to serious crime would need to be authorised by a judicial commissioner, with ministerial authorisation of warrants relating to national security being subject to judicial review.

30. Although they differed on much of the detail, particularly over the authorisation of warrants, it is telling that all three reviews found the current legislative framework provided by RIPA and other legislation to be essentially unfit for purpose and in need of replacement by a single piece of statute. This fundamental recommendation, which was accepted by the Government, had implications for the form of the Draft Investigatory Powers Bill, making it necessarily a wider and more far reaching document than its 2012 predecessor. Producing this document to a timescale which would fit with that already set by DRIPA required the Home Office and others within Government to carry out an exceptionally heavy workload at some pace. At points we have identified problems with the way the draft Bill is written and the timing and degree of the Government's consultation with stakeholders. These problems were hardly surprising given the sheer scale of the task to which the Government committed itself in the summer of 2015.

Publication of the draft Bill

31. The Home Office published its draft Bill, alongside a large amount of supporting information, on 4 November 2015. There were statements on the same day in both Houses. Speaking to the House of Commons, the Home Secretary, the Rt Hon Theresa May MP, outlined her view of the security context to the Bill:

> "The internet has brought us tremendous opportunities to prosper and interact with others. But a digital society also presents us with challenges. The same benefits enjoyed by us all are being exploited by serious and organised criminals, online fraudsters, and terrorists. The threat is clear. In the past 12 months alone, six significant terrorist plots have been disrupted here in the UK, as well as a number of further plots overseas. The frequency and cost of cyber-attacks is increasing, with 90% of large organisations suffering an information security breach last year. The Child Exploitation and Online Protection Centre estimates that there are 50,000 people in this country downloading indecent images of children.
>
> The task of law enforcement and the security and intelligence agencies has become vastly more demanding in this digital age. It is right, therefore, that those who are charged with protecting us should have the powers they need to

9 Royal United Services Institute (RUSI), *A Democratic Licence to Operate: Report of the Independent Surveillance Review*, July 2015

10 *Ibid.*

EMBARGOED until 09.30 on 11 February 2016

do so, but it is the role of Government and Parliament to ensure that there are limits to those powers."[11]

Concurrent parliamentary inquiries

32. As well as this Joint Committee, a number of other committees have been actively scrutinising the draft Bill. The Intelligence and Security Committee has been holding hearings to follow up its predecessor Committee's earlier report. The ISC is expected to publish its report at around the same time as this Committee. The Commons Science and Technology Committee conducted an inquiry into the technical aspects of the report and published its report on 1 February.[12] The Joint Committee on Human Rights invited evidence on the draft Bill and, although it has not commented at this stage, the Committee has indicated that it will scrutinise the Bill when it is ultimately introduced. Lastly at our request, and to a tight timescale, the Lords Delegated Powers and Regulatory Reform Committee examined the Government's draft delegated powers memorandum. Its views on the delegations are reproduced at Appendix 3.

33. We are conscious that the array of work in different committees, in addition to the primary role of this committee in addressing the draft Bill as a whole, had the potential to confuse rather than elucidate, and may have added to the burden on witnesses. The high degree of interest taken by committees shows the degree of importance Parliament attaches to these measures. This early and active engagement will no doubt assist the depth of scrutiny which Parliament can offer to the Bill proper when it comes.

What's in the draft Bill?

34. The arguments surrounding the capabilities provided by the draft Bill and the proposed authorisation and oversight arrangements are considered at length in the remainder of this report. The draft Bill is long and has a heavy technical element. We therefore hope it assists the reader to provide the below table, which simply describes each capability and explains where it is to be found in the draft Bill (clause numbers in parentheses).

EMBARGOED until 09:30 on 11 February 2016

11 HC Deb, 4 November 2015, col 969

12 House of Commons Science and Technology Committee, *Investigatory Powers Bill: technology issues* (Third Report, Session 2015–16, HC 573)

Table 1: The powers in the Draft Investigatory Powers Bill

Power	Conduct authorised	Statutory bodies/ purposes	Authorisation—Acquisition	Authorisation—Access	Oversight	Where addressed in this report
Targeted Interception (13)	Obtaining the content of a communication in the course of its transmission (12(2)(a))	5 law enforcement agencies, MI5, GCHQ, SIS and the Ministry of Defence (15(1))	Secretary of State authorisation, subject to approval by a Judicial Commissioner before non-urgent warrants come into force (14(1)(d))	N/A	Investigatory Powers Commission (IPC) (167) replaces the Interception of Communications Commissioner's Office (IOCCO), the Office of Surveillance Commissioners (OSC) and the Intelligence Services Commissioner (ISCom).	Capability: paras 34-42
	Obtaining related communications data (RCD) from communications described in the warrant (12(2)(b))	Purposes: National Security, Serious Crime, Economic Well-Being of the UK related to National Security and as part of a mutual assistance agreement (14(3))			The judge-led IPC will have an extensive remit to oversee the use of all investigatory powers and will scrutinise those provided with these powers though inspections, investigations, audits and	Authorisation: paras 434-444
Communications Data (CD) (46)	Obtain CD, usually via Communications Service Providers (CSPs) (46(2)) ('any person')	Public authorities provided with the ability to acquire CD (54) and statutory purposes (46(7)) listed in the Bill	Must be authorised by a designated person (who must be independent from the investigation) following consultation with a single point of contact (SPoC) (60)	N/A For ICRs, restricted to 3 specified purposes; local authorities excluded (47(4) and (5))		Capability: paras 43-88 (CD) and 89-156 (ICRs) Authorisation: paras 469-489

EMBARGOED until 09:30 on 11 February 2016

Power	Conduct authorised	Statutory bodies/ purposes	Authorisation—Acquisition	Authorisation—Access	Oversight	Where addressed in this report
Targeted Equipment Interference (EI) (81(1)(a))	Obtaining data covertly from computers and other equipment (communications, private information, equipment data—comms data, system data, extracted CD) (81, 82)	MI5, GCHQ, SIS, (84) law enforcement (89) and the Ministry of Defence (87) Purposes: National Security, Serious Crime and Economic Well-Being of the UK related to National Security. Law enforcement may only seek warrants for serious crime (89)	Secretary of State authorises warrants for MoD and security and intelligence agencies. (84, 87). Chief Constable authorises law enforcement use (89). All non-urgent warrants subject to Judicial Commissioner check before coming into force (84(1)(d), 87(1)(d), 89(1)(d))	N/A	authorisations of warrants and internal practices. (169, 170) Statutory Codes of Practice will outline further details (179)	Capability: paras 265-305 Authorisation: paras 445-452
Bulk Powers	Bulk interception (106) (obtaining overseas-re-lated content and related communications data (RCD) (106(2))	MI5, GCHQ, SIS (107(1)). Purposes: National Security, Serious Crime and Economic Well-Being of the UK related to National Security (107(1)/(2))	Secretary of State authorises warrants, subject to approval by a Judicial Commissioner (107, 137, 122) Interception and equipment interference warrants (but not data acquisition	Examination of any material must be necessary for a specified Operational Purpose (which can be general (111(4)), 140(5)), 125(4)), authorised by a Secretary of State and approved by a Judicial		Capability: paras 306-374 Authorisation: paras 490-493

EMBARGOED until 09:30 on 11 February 2016

Power	Conduct authorised	Statutory bodies/ purposes	Authorisation—Acquisition	Authorisation—Access	Oversight	Where addressed in this report
	Bulk Equipment interference (135)(1)(b) Obtaining overseas-related stored communications, private information and equipment data other equipment (135, 136)	MI5, GCHQ, SIS (137(1). Purposes: National Security Serious Crime and Economic Well-Being of the UK related to National Security. (137(1)/(2))	warrants) must be for overseas-related information. (106, 135)	Commissioner. Examination of content relating to persons in the UK requires a separate targeted examination warrant	*see above*	*see above*
	Bulk acquisition of Communications data (122)	MI5, GCHQ, SIS (122(1)). Purposes: National Security, Serious Crime and Economic Well-Being of the UK related to National Security. (122(1)/(2))				

EMBARGOED until 09:30 on 11 February 2016

Power	Conduct authorised	Statutory bodies/ purposes	Authorisation—Acquisition	Authorisation—Access	Oversight	Where addressed in this report
Bulk Personal Datasets (BPD) (150)	Warrants authorising the obtaining, retention and examination of classes of BPDs (153) and specific BPDs (154).	MI5, GCHQ, SIS (153(1), 154(1)) Purposes: National Security, Serious Crime and Economic Well-Being of the UK related to National Security (153(3), 154(5))	Authorisation to acquire BPDs issued by Secretary of State and subject to approval by a Judicial Commissioner (153(3), 154(5))	Examination of any material must be necessary for a specified Operational Purpose (153 (4), 154 (4)), authorised by a Secretary of State and approved by a Judicial Commissioner	*see above*	Capability: paras 375-408 Authorisation: paras 494-497
Data retention notices (71)	Imposing a requirement on a telecommunications operator to retain relevant communications data (71)	The Secretary of State considers it necessary and proportionate (71 (1)) for any of the purposes listed in 46(7)	The Secretary of State considers it necessary and proportionate (71 (1))	Access is through the power to obtain communications data (46)	An appeal to the Secretary of State against a Data retention notice requires the Secretary of State to consult the Technical Advisory Board and the Investigatory Powers Commissioner (73(6))	Capability: paras 157-229

EMBARGOED until 09:30 on 1 February 2016

Power	Conduct authorised	Statutory bodies/ purposes	Authorisation—Acquisition	Authorisation—Access	Oversight	Where addressed in this report
National Security notices (188)	Serving a notice requiring a tel-ecommunica-tions operator to take any steps necessary in the interests of national security (188(1))	Purposes: Necessary in the interests of national security (188(1))	The Secretary of State must consider the notice to be proportionate (188(2)) Notices may not require the taking of any steps the main purpose of which would be to do something for which a warrant under the other provisions of the Bill would be required (188(4)).	N/A	An appeal to the Secretary of State against a National Security notice requires the Secretary of State to consult the Investigatory Powers Commissioner (191 (5))	Authorisation: paras 498-502
Technical Capability notices (189)	Imposing specific obligations on providers of postal or telecommunica-tions services (189 (2))	Purposes: Obliging postal or telecommu-nications service providers to provide particular services, handle material and remove electronic protections from material (189 (4))	The Secretary of State must consider the notice to be reasonable and practicable (189 (3)) and consult with the Technical Advisory Board and the person upon whom the obligations fall (189 (5))	N/A	An appeal to the Secretary of State against a Technical Capability notice requires the Secretary of State to consult the Technical Advisory Board and the Investigatory Powers Commissioner (191 (5))	Capability: paras 248-264 (encryption) Authorisation: paras 498-502

The information in this table has been based on the information provided in the submission by Professor Lorna Woods on behalf of an *ad hoc* working group on the draft Bill.[13]

13 Written evidence from Lorna Woods (IPB0163)

EMBARGOED until 10:30 on 11 February 2016

3 Capabilities

Overview

35. This Chapter addresses the investigatory powers and capabilities that the draft Bill proposes for law enforcement and the security and intelligence agencies. It outlines whether these powers are new and, if not, where they are currently legislated for. It examines the purposes for which these powers are sought and considers whether they are appropriate, legal and technically feasible to deliver.

36. Subsequent chapters discuss the warrant authorisation processes for these powers and the oversight regimes to which they would be subjected.

Targeted Interception

37. Part 2 of the draft Bill provides for targeted interception to be carried out by law enforcement and the security and intelligence agencies.

38. Interception is described by the Home Office as "the making available of the content of a communication—such as a telephone call, email or social media message—in the course of its transmission or while stored on a telecommunications system."[14] Targeted interception is an existing power available to law enforcement and the security and intelligence agencies under Part 1 Chapter 1 of RIPA.

The case for Targeted Interception

39. The Committee was told by law enforcement that interception "is used as a source of intelligence which assists in identifying and disrupting threats from terrorism and serious crime."[15] They said that their use of interception is "tightly targeted", provides "significant operational benefits" and "is likely to remain of vital importance".[16]

40. The evidence received by the Committee supported the continued use of targeted interception.[17] Ray Corrigan said "The government has the right to intercept, retain and analyse personal information, when someone is suspected of a serious crime",[18] while the Open Rights Group said "Targeted interception of communications under strict conditions has a place in a democratic society."[19]

41. The concerns raised by witnesses about targeted interception related to the terms of the warrants authorising this activity, which are addressed in Chapter 4, and the term "related communications data", which is discussed in the section on bulk interception. Additionally, considerations of the admissibility of intercept evidence in legal proceedings and the need for a definition of national security are considered in Chapter 6.

42. **We agree that the targeted interception power should be part of the Bill, subject to appropriate warrant authorisation arrangements.**

14 Home Office, *Draft Investigatory Powers Bill: Guide to Powers and Safeguards*, Cm 9152, November 2015, p.8
15 Written evidence from law enforcement (IPB0140)
16 *Ibid.*
17 See, for example, written evidence from Howard Clark (IPB0070) and Liberty (IPB0143)
18 Written evidence from Mr Ray Corrigan (IPB0053)
19 Written evidence from Open Rights Group (IPB0108)

EMBARGOED until 09:30 on 11 February 2016

Communications Data

43. Part 3 of the draft Bill provides for the acquisition of communications data by law enforcement and the security and intelligence agencies.

44. Communications data is information about communications. The Home Office describe it as "the 'who', 'where', 'when', 'how' and 'with whom' of a communication but not what was written or said."[20]

45. Communication Service Providers (CSPs) can currently be required to keep communications data for up to 12 months under the Data Retention and Investigatory Powers Act 2014 (DRIPA) when it has been deemed necessary and proportionate. Law enforcement and the security and intelligence agencies may acquire that data under the processes set out in RIPA sections 21–25.

The background to Communications Data

46. It is useful to understand how Communications Data has developed.[21] Historically "communications data" was obtained from telephone companies. Companies offering traditional landline based services routinely generate records which show which numbers called each other, when and for how long. These are used as the basis for charging customers and for sharing revenue with other telephone companies where there are inter-connects. Because those companies also have information about their customers through their contracts, the data includes "who was calling whom".

47. The information generated by the telephone companies is called Call Data Records (CDRs). In the case of mobile phone companies, additional data is routinely collected. As well as which numbers were calling which, when and for how long, the data also includes the hardware identity of the phone—its IMEI—and of the SIM installed within it—the IMSI. More importantly it captures the identity and hence the location of the mast to which the phone is registered. The global mobile phone system needs to know the location of each phone so that incoming calls can be diverted to it via the radio mast that has the strongest signal; registration and re-registration takes place constantly for so long as a mobile phone is powered up. This geo-location data, once in the hands of investigators, can be used to track the movements of the user of a mobile phone in a technique called "cell site analysis". The main limitation on the value of mobile phone call data records for investigative purposes is that the actual users of the phones may not be the individuals who had originally purchased them. But correlating techniques can, with some success, be deployed to overcome attempts at user anonymity.

48. As communications patterns have moved from primarily calls and SMS text messages to a wide range of internet activity, Government has sought to maintain the capabilities of law enforcement in this new sphere.

The case for Communications Data

49. The Home Office and law enforcement emphasised in their evidence the importance of communications data to criminal investigations and prosecutions. Paul Lincoln, Director,

20 Home Office, *Draft Investigatory Powers Bill: Guide to Powers and Safeguards*, Cm 9152, November 2015, p.12
21 We are particularly grateful for the input of our specialist advisers for this section.

EMBARGOED until 09:30 on 11 February 2016

National Security (Office for Security and Counter-Terrorism) at the Home Office told the Committee that:

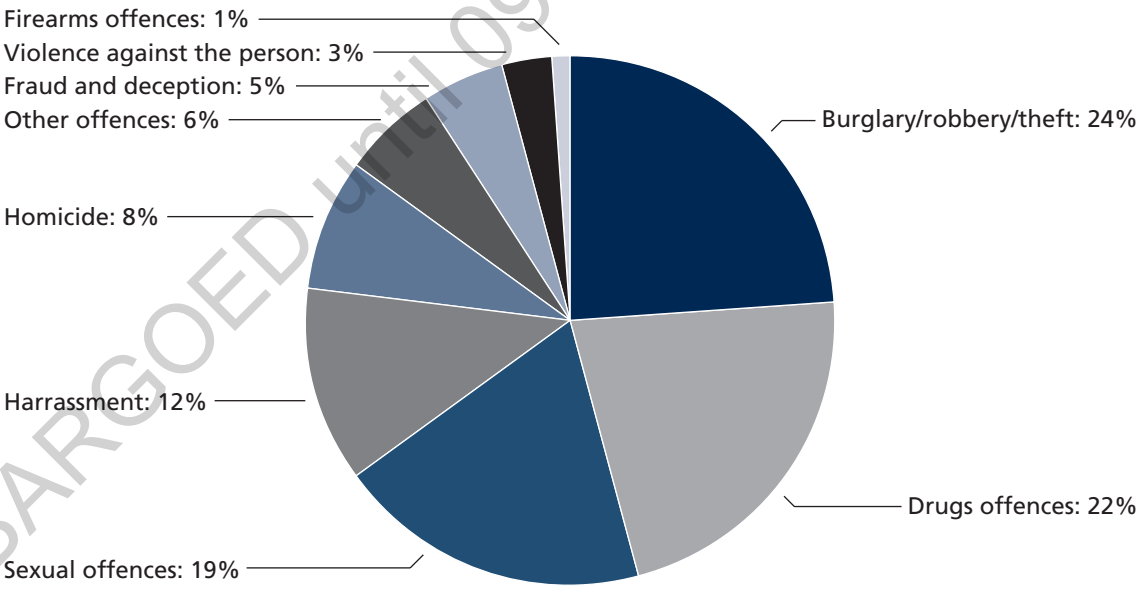
> "It is an essential tool for law enforcement in particular to identify, for example, missing persons or to rule people out of an investigation and try to minimise more intrusive techniques to gain content from that. It is very valuable."[22]

50. In a similar vein, Assistant Chief Constable Richard Berry from the National Police Chiefs' Council said:

> "It is essential, for example for establishing a lead, a seed upon which to build an inquiry. For example, if we take stalking and harassment, which is a very topical issue, around domestic abuse victims. To be able to establish a particular communication and an evidential line of inquiry around a victim being stalked, would be incredibly useful, in fact—vital, to support and corroborate an allegation."[23]

51. Statistics about the usage of communications data demonstrate that it is used extensively for such purposes. Jo Cavan, Head of the Interception of Communications Commissioner's Office (IOCCO), told the Committee that "Around 500,000 requests for communications data are made on an annual basis".[24] A recent analysis by IOCCO of 100,000 communications data applications provides a breakdown by crime type (see Figure 1).

Figure 1: Breakdown of 100,000 Communications Data Applications submitted under section 22(2)(b) RIPA by Crime Type



Source: Interception of Communications Commissioner's Office, *Senior Responsible Officer Circular (4) Breakdown of communications data applications under s22(2)(b) RIPA by crime type*, 20 November 2015.

52. Simon York, Director of the Fraud Investigation Service at Her Majesty's Revenue and Customs (HMRC), provided an insight into how HMRC used communications data:

22 Q 14 (Paul Lincoln, Home Office)
23 Q 28 (Assistant Chief Constable Richard Berry, National Police Chiefs' Council)
24 Q 48 (Jo Cavan, Interception of Communications Commissioner's Office)

EMBARGOED until 09:30 on 14 February 2016

> "Last year, we made just over 10,000 communications data requests. That supported 560 investigations. I think that those numbers represent the complexity and the conspiracy involved in many of these cases. Almost 100% of our requests were in relation to preventing and detecting crime … This can be in relation to anything from smuggling to tax fraud to trying to criminally exploit HMRC's repayment systems. Literally billions of pounds are at stake here. Last year, investigations where we used communications data and intercept together prevented around £2 billion loss to the UK Exchequer. That is how important it is to us. "[25]

53. The Crown Prosecution Service emphasised the importance of communications data in pursuing prosecutions, telling the Committee that "It has played a significant role in every Security Service counter-terrorism operation over the last decade and is used in 95% of serious and organised crime prosecutions."[26]

54. There was support for accessing communications data from beyond the voices of government and law enforcement, with the Information Commissioner's Office, Liberty, NSPCC, and Lord Carlile of Berriew CBE QC all noting the importance of communications data to modern policing.[27]

The intrusiveness of communications data and privacy risks

55. The Committee did not hear concerns that the existing use of communications data was problematic in principle. The issues raised by witnesses were not that communications data was not useful or important to tackling crime, but that the retention and accessing of such data is intrusive and has considerable privacy implications.

56. Accessing communications data has historically been perceived to be a less intrusive investigative tool than accessing the content of a communication. While interception would expose the content of a message, communications data revealed only that a communication had taken place. As Liberty explained, technological developments have made this distinction less straightforward:

> "At one time a firm distinction between communications data and content would have been more credible, for example when much communication was by letter: everything inside the envelope is content, everything on the outside communications data. However, this distinction has been eroded by the scale of modern internet and mobile phone usage."[28]

57. Witnesses with concerns about communications data argued it was either more intrusive than accessing content or, in the words of Dr Paul Bernal, not less intrusive but "differently intrusive".[29] The basis for these concerns related to the potential intrusiveness of Internet Connection Records (a new form of communications data) and the potential for bulk analysis of aggregated communications data. These issues will be examined further

EMBARGOED until 09:30 on 11 February 2016

25 Q 30 (Simon York, HMRC)
26 Written evidence from the Crown Prosecution Service (IPB0081)
27 Written evidence from Lord Carlile of Berriew CBE QC (IPB0017), the NSPCC (IPB0049), the Information Commissioner's Office (IPB0073) and Liberty (IPB0143)
28 Written evidence from Liberty (IPB0143)
29 Written evidence from Dr Paul Bernal (IPB0018)

in the relevant sections later in this Chapter and the appropriate level of authorisation for accessing communications data is considered in Chapter 4.

58. **We agree that the power to obtain communications data is an important tool for law enforcement and other public bodies. It should be included in the Bill.**

Definitions of communications data

59. One of the most common concerns among witnesses was the definitions of communications data and content that are proposed in the draft Bill to replace the terminology used in RIPA section 21(4).[30] It is necessary to define categories of communications data so that applications for more intrusive categories of material can be examined and authorised by officials of a higher seniority.

Box 1: Defining Communications Data in RIPA

The challenge of defining communications data first arose during consideration of what became the Regulation of Investigatory Powers Act 2000 and in the versions of the Code of Practice on the Acquisition and Disclosure of Communications Data that followed. These currently define communications data as:

- traffic data (as defined by sections 21(4)(a) and 21(6) of RIPA)—this is data that is or has been comprised in or attached to a communication for the purpose of its transmission;
- service use information (as defined by section 21(4)(b) of RIPA)—this is the data relating to the use made by a person of a communications service; and
- subscriber information (as defined by section 21(4)(c) of RIPA)—this relates to information held or obtained by a CSP about persons to whom the CSP provides or has provided a communications services. Those persons will include people who are subscribers to a communications service without necessarily using that service and persons who use a communications service without necessarily subscribing to it.

Traffic data includes data identifying a computer file or a computer program to which access has been obtained, or which has been run, by means of the communication—but only to the extent that the file or program is identified by reference to the apparatus in which the file or program is stored. In relation to internet communications, this means traffic data stops at the apparatus within which files or programs are stored, so that traffic data may identify a server or domain name (web site) but not a web page. For example, the fact that a subject of interest has visited pages at http://www.gov.uk/ can be acquired as communications traffic data (if available from the CSP), whereas that a specific webpage that was visited is http://www.gov.uk/government/collections/ripa--forms-2 may not be acquired as communications data (as it would be content). This is sometimes informally referred to as the "up to the first slash" rule.

The Code of Practice highlights two common specific situations: for emails—the "headers" which can include, "from", "to" and "date" information but not the "subject"

EMBARGOED until 09.30 on 11 February 2016

30 Home Office, *Acquisition and Disclosure of Communications Data Code of Practice*, March 2015

and not the message itself; for web-browsing "information to the extent that only a host machine, server, domain name or IP address is disclosed" .

Service Use information "is, or can be, routinely made available by a CSP to the person who uses or subscribes to the service to show the use of a service or services and to account for service charges over a given period of time." (Code of Practice, paragraph 2.29).

Subscriber information is, essentially, "who owns that phone" and "who had that IP address at that time?"

Almost the only type of Internet activity that is easily interpreted as communications data and captured is conventional email traffic. Here the standards for email headers ensure that the "communications data" will always appear in the same place and can therefore be readily extracted by means of a simple parsing computer program. Almost everything else that investigators are likely to desire comes across the "up to the first slash" limitation. This applies to webmail, bulletin boards, many instant message services and many social networking services as well. Similar difficulties apply to cloud based services, whether these are used simply to store data or to process it. These problems also apply to mobile apps; access to third party and over-the-top services may not take place via a computer that looks like a web-server as with conventional PC operation, but Internet-connected computers are involved which provide a gateway to further communications.

60. Communications data is defined in Clause 193 as "entity" or "events" data about a communication, which does not include the content of that communication. "Entity data" is defined as information about an entity and how it relates to a telecommunications system, while "Events data" is data about events that take place on that system involving entities. The explanatory notes to the Bill provide examples of entity data (phone numbers or IP addresses) and events data (the fact that someone has sent or received an email or text message, a record of the entities involved in a phone call or the location a mobile phone call). Finally, content is defined as "anything of what might reasonably be expected to be the meaning of the communication".

61. There was support for the new definitions from the British Computer Society (BCS), The Chartered Institute for IT, who said that:

> "the terms employed and the process proposed by the draft Bill to capture and where necessary share communication data with the appropriate organisations, and people within those organisations to be well defined and workable … BCS believes the definitions of content and communications data (including the distinction between 'entities' and 'events') are sufficiently clear and practical for the purposes of accessing such data."[31]

62. From a legal perspective, the Crown Prosecution Service said that "the new definitions are both sufficiently clear and viable. The draft Bill makes a helpful contribution to

31 Written evidence from BCS, The Chartered Institute for IT (IPB0075)

EMBARGOED until 09:30 on 11 February 2016

clarifying what is currently a complex area."[32] This view was supported by the Serious Fraud Office.[33]

63. Other witnesses challenged the clarity and effectiveness of these definitions. Privacy International argued that "The definitions of entity and events data are too vague and fail to take into account the distinctions that may arise in the types of data generated by modern technology. For instance, data about a phone call over landline (e.g. two BT numbers shared a connection for 13 minutes) is vastly different than each 'event' within a chat session."[34]

64. Other evidence suggested that separating communications data from content was not feasible. F-Secure said that "From the network technology point of view, the definitions are not practical to allow for different courses of action to take place dependant on whether the data is classed as entity or event. There is a significant amount of crossover between entities and events."[35]

65. Open Intelligence told the Committee that "On a technical level distinguishing between content and communications data as far as web use is concerned is questionable, not least because an Internet connection is most often being used for multiple services simultaneously, with data packets mixed together."[36] The ability to distinguish between content and communications data is particularly important because of the separate regimes for authorisation and the fact that interception of content and its associated methods is inadmissible in legal proceedings. This issue is also relevant to Internet Connection Records (paras 89–156).

66. The definition of content was also a concern for witnesses. Dr Paul Bernal questioned the reference to "meaning" in the definition of content, saying "It is possible to derive 'meaning' from almost any data—this is one of the fundamental problems with the idea that content and communications can be simply and meaningfully separated. In practice, this is far from the case."[37] Graham Smith posed a challenging philosophical and technical question, "For a computer to computer communication, what is the meaning of 'meaning'?"[38]

67. The written evidence provided by the Home Office set out in greater detail types of communications data and content for different forms of communication—postal, mobile telephony, internet access and internet applications.[39] Unfortunately this information arrived too late for many witnesses to give the Committee their views on whether it provided sufficient clarity on the definitions.

68. **We acknowledge the difficulty of providing definitions broad enough to capture the variety of ways in which communications are conducted, and may be conducted in the future, while still providing sufficient clarity and precision.**

EMBARGOED until 09:30 on 11 February 2016

32 Written evidence from the Crown Prosecution Service (IPB0081)
33 Written evidence from the Serious Fraud Office (IPB0153)
34 Written evidence from Privacy International (IPB0120)
35 Written evidence from F-Secure Corporation (IPB0118)
36 Written evidence from Open Intelligence (IPB0066)
37 Written evidence from Dr Paul Bernal (IPB0018)
38 Written evidence from Graham Smith (IPB0126)
39 Written evidence from the Home Office (IPB0146) Annex A

69. ***We are grateful that the Government has provided further information on the interpretation of communications data and content. We have not had an opportunity to seek views as to whether the definitions are now sufficiently clear. Parliament will need to look again at this issue when the Bill is introduced. We urge the Government to undertake further consultation with communications service providers, oversight bodies and others to ascertain whether the definitions are sufficiently clear to those who will have to use them. (Recommendation 1)***

70. LINX explained that the definition of entities had its roots in the "subscriber data" definition in RIPA, which in practice meant "the information that a telecommunications operator held about their customer, such as their name and address, and other relatively unintrusive information regarding the services taken and billing."[40] They argued that new term "entity data" was "exceptionally broad" as it no longer referred only to customers, but could include anyone interacting over a telecommunications operator's network.[41] LINX also suggested that the breadth of "entity data" would be wider still due to the new definition of telecommunications operators (which is examined further in the Data Retention section):

> "Amongst the types of companies that now fall within the new definition of a telecommunications operator [are] social networking sites and online messaging services. This means that Apple, Facebook, Google, Microsoft, Yahoo! and others will all be considered telecommunications operators within the meaning of the Draft Bill. And everything they know about anyone will be considered "entity data", other than that which is events data." [42]

71. Dr Paul Bernal said that communications data "is by nature of its digital form ideal for analysis and profiling. Indeed, using this kind of data for profiling is the heart of the business models of Google, Facebook and the entire internet advertising industry."[43]

72. Given the sophisticated automated profiling of users that such companies undertake as a core part of their businesses, it is not hard to see how the "entity data" they hold would be considerably more detailed, and thus more intrusive, than the "subscriber information" that was originally envisaged when RIPA received Royal Assent.

73. **We are concerned about the potential detail that entity data might encompass in relation to telecommunications providers, such as Facebook and Google, who build detailed automated profiles of their users. The Government should say whether it wishes to acquire such data in principle and, if not, how it will ensure that the entity data it requests and receives is not of that level of detail.**

74. Another concern among many witnesses was the definition of "data" in Clause 195, which states that "In this Act "data" includes any information which is not data". Open Intelligence described this as "obvious paradoxical nonsense"[44] and Graham Smith suggested that it would "surely invite comparisons with the impenetrability of RIPA."[45]

75. The Home Secretary in her evidence appeared to acknowledge the point:

40 Written evidence from LINX (IPB0097)
41 *Ibid.*
42 *Ibid.*
43 Written evidence from Dr Paul Bernal (IPB0018)
44 Written evidence from Open Intelligence (IPB0066)
45 Written evidence from Graham Smith (IPB0126)

EMBARGOED until 09:30 on 11 February 2016

> "I completely understand people raising an eyebrow or two at that particular sentence, which I did when I read it myself. I am happy to look at the wording, but it is an attempt to do something very simple. If you talk about data, a lot of people tend to think only about computer stuff—electronic records. We are saying that when we use the term "data" in the Bill it can cover, for example, paper records as well. It is an attempt to be helpful, which, in its language, it has not been."[46]

76. ***The definition of data in Clause 195 is unclear, unhelpful and recursive. The Government must provide a meaningful and comprehensible definition of data when the Bill is introduced. (Recommendation 2)***

Public bodies who may obtain communications data

77. The draft Bill provides for a large number of public bodies to apply to access communications data. These are listed in Schedule 4. Paul Lincoln from the Home Office explained that:

> "A wide range of bodies have access to communications data. The Financial Conduct Authority might use it for conducting investigations into insider trading. The Maritime and Coastguard Agency might use it for finding missing people at sea. For local authorities, ways in which to investigate might include rogue traders, environmental offences or benefit fraud. David Anderson said that if you have relevant criminal investigation powers you should have the tools associated with that, and communications data is one of them."[47]

78. Mr Lincoln also said that local authorities were relatively small users of communications data, accounting for 0.5% of the requests made for communications data overall. [48]

79. Local authorities and trading standards will continue to have the power to request communications data under the draft Bill.[49] The Convention of Scottish Local Authorities (COSLA) explained that:

> "local authority access to communications data is vital in ensuring that criminal investigations into serious matters such as illegal money lending, doorstep crime and intellectual property offences can be progressed and brought to a successful conclusion. Local authorities do not make a large number of applications for communications data and the small number of applications that are rejected shows that, when they do so, it is in a proportionate and appropriate manner."[50]

80. Further evidence from the Local Government Association, National Anti-Fraud Network, Chartered Trading Standards Institute and Association of Chief Trading Standards Officers and from Trading Standards North West also argued strongly for the continued right of local authorities to access communications data.[51]

46 Q 261 (Theresa May MP)
47 Q 15 (Paul Lincoln, Home Office)
48 Q 18 (Paul Lincoln, Home Office)
49 They will not, however, have access to Internet Connection Records. See Clause 47(5).
50 Written evidence from the Convention of Scottish Local Authorities (COSLA) (IPB0042)
51 Written evidence from the Local Government Association (LGA), National Anti-Fraud Network (NAFN), Chartered Trading Standards Institute and Association of Chief Trading Standards Officers (IPB0051) and Trading Standards North West (IPB0092)

EMBARGOED until 09.30 on 11 February 2016

81. While the Committee is aware that concerns have been raised about the use of communications data by local authorities, the evidence received did not reflect such concerns. We note that local authorities will not have access to the potentially more intrusive Internet Connection Records.

82. **We agree that local authorities and trading standards should continue to have access to communications data to support their law enforcement roles, but this intrusive power should not be used for minor infringements.**

83. ***We recommend that Parliament should give further consideration to defining the purposes for which local authorities may be allowed to apply for communications data when the Bill is introduced. (Recommendation 3)***

Purposes for which communications data may be obtained

84. Clause 46 (7) of the draft Bill sets out the purposes for which communications data may be obtained by those authorised to do so, where necessary and proportionate.

85. Law enforcement (LE) raised a concern regarding Clause 46 (7)(g) which allows for communications data (CD) (other than Internet Connection Records) to be obtained, where necessary and proportionate, for the purpose of preventing death, injury or damage to a person's physical or mental health in an emergency:

> "It is within this 'emergency' category where there may be potential difficulties. Hundreds of people are reported as missing in the UK every year, many of them are classed as vulnerable due to their age or mental or physical health and LE would rightly seek to limit the danger to which such individuals are exposed by locating them as soon as reasonably practicable. Not all instances would be deemed an 'emergency' and it is unclear why CD cannot be used as a tool of early consideration rather than meeting the requirements of last resort to prevent harm to an individual. LE believes that 'saving life' should be explicitly available as a justification to avoid emergency situations."[52]

86. The Home Secretary in her evidence said that in her view that saving life constituted an emergency and that there would be no undue restriction of law enforcement's use of communications data in this regard:

> "The definition of an emergency will cover a whole range of circumstances where the police will suspect that somebody is in danger and that there is a requirement for them to access this data. That is why I have been comfortable with using that phrase in terms of the emergency. I have tested with my officials certain circumstances where saving a life might arise, and I think in all those that I have looked at it would be covered by the definition of emergency. Almost by definition, if the police or another authority are trying to intervene to save a life, that is an emergency circumstance."[53]

87. ***We believe that law enforcement should be able to apply for all types of communications data for the purposes of 'saving life'. We recommend that the Home Office should undertake further consultation with law enforcement to determine***

52 Written evidence from law enforcement (IPB0140)
53 Q 262 (Theresa May MP)

EMBARGOED until 09:30 on 11 February 2016

whether it is necessary to amend Clause 46 (7)(g) to make this explicit on the face of the Bill. (Recommendation 4)

88. A related issue on the purposes for which Internet Connection Records may be accessed is considered in paras 151–156.

Internet Connection Records

89. Clause 47 introduces a new power to collect and access Internet Connection Records (ICRs). Internet Connection Records are an extension of communications data that the Government has said is essential to maintain the investigate capabilities of law enforcement in the digital age. In the words of the Home Office, "Without ICR retention, it remains impossible for law enforcement to identify consistently who has sent a particular communication online."[54]

90. The Government is seeking to address two problems with ICRs. The first is IP address resolution; identifying which device is communicating with which other device. This is not a straightforward task, as a single public IP address may be used by multiple people at once (for example, people sharing a WiFi connection in a coffee shop) and by different people at different times (using dynamic IP addresses). The shortage of available IPv4 addresses and the techniques used to work around this, such as Carrier-Grade Network Address Translation and Port Address Translation, are also a significant complicating factor.[55]

91. The second problem is that, even with the originating and destination IP addresses, it may not be clear what website or communications service a person is accessing. This can be due to shared webhosting, cloud computing services and content delivery networks.[56] For example, under existing arrangements it is only possible to see that someone has accessed a webmail site such as Gmail or Hotmail, or a social networking site such as Facebook. But further communication will often have taken place from those websites. The same applies to many smartphone applications.

92. For a further discussion of the technical issues, see the report of the House of Commons Science & Technology Committee.[57]

The case for ICRs

93. The Home Office told the Committee that ICRs would be essential to maintain existing levels of capability for law enforcement, in light of the changing technologies and communications patterns that have been outlined above. Paul Lincoln said that "In terms of the powers and capabilities, a new capability [ICRs] is provided for that in effect restores powers that used to exist."[58]

EMBARGOED until 09:30 on 11 February 2016

54 Home Office, *Operational Case for the Retention of Internet Connection Records*, 4 November 2015

55 This issue may be ameliorated by the adoption of IPv6, although progress has so far been limited and widespread deployment and usage is not imminent.

56 See, for example, written evidence from Christopher Lloyd (IPB0056), Ian Batten (IPB0090) and Electronic Frontier Foundation (IPB0119)

57 House of Commons Science and Technology Committee, *Investigatory Powers Bill: technology issues* (Third Report, Session 2015–16, HC 573)

58 Q 1 (Paul Lincoln, Home Office)

94. The Home Office said in their operational case that "Rapid technological change means that law enforcement's inability to access online CD is significant and will only get worse if it continues to be impossible to require communications companies to retain ICRs. More and more communications are taking place over the internet and as this happens it follows that an increasing proportion of CD will be unavailable when it is needed."[59]

95. There was support for this position from law enforcement, who said that "full ICR retention is imperative to the ability to enable IP address resolution for retrospective investigations".[60] The Crown Prosecution Service agreed, saying "the benefits of the contribution ICRs could make in enabling investigators to identify suspects are evident."[61]

96. Michael Atkinson, Secretary to the National Police Council's Data Communications Group, told the Committee that:

> "I have spent several hours in one of the UK CSPs for mobile phones … What I can say is that they are assuring me that, without the retention of ICRs, they will not be able to solve internet protocol resolutions. They also tell me that we will not get the evidence that we need in order to undertake further investigations of people who may be of interest to us.[62]

97. Other witnesses beyond law enforcement supported the proposal for ICRs. The NSPCC said that "existing evidence suggests that this is a necessary expansion of existing capabilities"[63], while the BCS said that "accessing ICR is essential for identifying the sender of an online communication, identifying which ISP is being used and where and when illegal content has been accessed."[64]

The case against ICRs

98. A number of witnesses opposed ICRs on the basis that they were too intrusive. Big Brother Watch told the Committee that "Analysing our internet history or what sites we have visited can provide a rich source of extremely revealing data which can be used to profile or create assumptions about an individual's life, connections and behaviour."[65]

99. Dr Tom Hickman suggested that:

> "A key danger in enabling access to ICR is that it could allow authorities to identify suspect web-browsing patterns, perhaps in combination with other communications data, in order to identify suspect categories of person (internet records includes information about the "pattern" of communications). This is different from using such data to identify known (but unidentified) suspects."[66]

100. Caroline Wilson Palow, Privacy International, discussed privacy concerns about accessing the domain name up to the first slash:

59 Home Office, Operational Case for the Retention of Internet Connection Records, 4 November 2015
60 Written evidence from law enforcement (IPB0140)
61 Written evidence from the Crown Prosecution Service (IPB0081)
62 Q 164 (Michael Atkinson, National Police Council's Data Communications Group)
63 Written evidence from the NSPCC (IPB0049)
64 Written evidence from BCS, The Chartered Institute for IT (IPB0075)
65 Written evidence from Big Brother Watch (IPB0007)
66 Written evidence from Dr Tom Hickman (IPB0039)

EMBARGOED until 09:30 on 11 February 2016

> "Potentially, that could be quite intrusive and could reveal a whole lot of information. It is not as innocuous as just bbc.co.uk, which is the example that they gave. For instance, that domain name could be saveyourmarriagelikeme.net or domesticviolenceservices.com. Maybe one of the most interesting ones is crimestoppers-uk.org. This is where you can make anonymous tips to help to solve crimes. Of course, if you had the Internet connection record that said that someone had gone to crimestoppers-uk.org and you also knew the time when the tip had come in—if you were the police, for instance—you could very easily figure out who had put in that tip. That is a real problem, because if you are destroying that anonymity you can undermine the ability to solve crime."[67]

101. The IT-Political Association of Denmark, said:

> "Collection of ICR information will be extremely intrusive to the private lives of British citizens. The destination IP addresses will, in some cases, contain sensitive information about political and religious preferences of citizens through their choices of online news media, visits to websites of political parties and candidates as well as religious groups and societies. The health conditions of citizens could be revealed through the frequency of visits to websites with information about specific diseases and medical conditions, even when the individual web pages (URLs) are not retained."[68]

102. Similar points were made by Dr Paul Bernal, Daniel Walrond, Scottish Pen, Open Rights Group, F-Secure Corporation, Privacy International, Dr Julian Huppert and Liberty.[69]

103. TalkTalk raised a practical consequence of ICRs with privacy implications. They explained that section 7 of the Data Protection Act 1998 allows individuals to request a copy of the information an organisation holds about them, a process commonly referred to as a subject access request. They said that:

> "Privacy issues must also be carefully considered, as the data would relate to each individual who has used an internet connection, not just the account holder. In the case of an internet connection record, this would allow customers to potentially see data relating to the browsing habits of a spouse or housemate, which has significant privacy implications."[70]

104. TalkTalk also pointed out that providing this information would also be a technical challenge for CSPs, given the volume of data involved.[71]

105. Alongside the objections to ICRs in principle, the Committee received considerable evidence about the practicality of this proposal. These issues are considered below.

106. **We consider that, on balance, there is a case for Internet Connection Records as an important tool for law enforcement. We have concerns about the definitions and**

EMBARGOED until 09:30 on 11 February 2016

67 Q 130 (Caroline Wilson Palow, Privacy International)
68 Written evidence from the IT-Political Association of Denmark (IPB0103)
69 Written evidence from Dr Paul Bernal (IPB0018), Daniel Walrond (IPB065), Scottish PEN (IPB0076), Open Rights Group (IPB0108), F-Secure Corporation (IPB0118), Privacy International (IPB0120), Dr Julian Huppert (IPB0130) and Liberty (IPB0143).
70 Written evidence from TalkTalk (IPB0154)
71 *Ibid.*

feasibility of the existing proposal, which the Home Office must address. These are set out in the following sections. It is also important for ICRs to be properly authorised and overseen, and these issues will be considered in subsequent chapters.

107. ***We recommend that the Government should publish in a Code of Practice alongside the Bill advice on how data controllers should seek to minimise the privacy risks of subject access requests for ICRs under the Data Protection Act 1998. (Recommendation 5)***

108. ***While we recognise that ICRs could prove a desirable tool for law enforcement agencies, the Government must address the significant concerns outlined by our witnesses if their inclusion within the Bill is to command the necessary support. (Recommendation 6)***

The definition of ICRs

109. Many witnesses raised concerns with the Committee that the definition of ICRs was vague, both in terms of what information would be collected and who would collect it. Witnesses emphasised that ICRs did not currently exist, were not a recognised term in the industry and did not refer to datatypes recognised by internet engineers.[72] In the view of the Open Rights Group, "they are not properly defined and introduce excessive uncertainty."[73]

110. The Internet Service Providers' Association (ISPA) told the Committee that "The Investigatory Powers Bill does not provide a clear definition of ICRs making it difficult to assess what data could fall under the definition and what impact the collection of this data may have on businesses and consumers."[74]

111. Dr Paul Bernal argued that:

> "This definition is vague, and press briefings have suggested that the details would be in some ways negotiated directly with the communications services. This does not seem satisfactory at all, particularly for something considered to be such a major part of the Bill"[75]

112. The Center for Democracy & Technology told the Committee that:

> "The definitions in the Draft Bill are insufficiently narrowly defined. Definitions should be drafted to map unambiguously onto current features of Internet architecture and protocols so that communications service providers (CSPs) can understand what they will need to collect, retain and be prepared to produce with the proper legal authorisation. We recognise the importance of ensuring that technological developments do not render the powers detailed in the bill ineffective. However, in our view the terminology is currently so broad that there is not only difficulty in mapping the legislative language to

EMBARGOED until 09:30 on 11 February 2016

72 See, for example, written evidence from Andrews & Arnold Ltd (IPB0001), the IT-Political Association of Denmark (IPB0103) and GreenNet Ltd (IPB0132), Q 105 (Hugh Woolford, Virgin Media) and Q 152 (Jonathan Grayling, EE)
73 Written evidence from Open Rights Group (IPB0108)
74 Written evidence from ISPA (IPB0137)
75 Written evidence from Dr Paul Bernal (IPB0018)

> actual features of existing technology, but also real uncertainty created with respect to the scope of the powers sought in the Bill."[76]

113. Graham Smith, in evidence submitted to the House of Commons Science and Technology Committee, pointed out that the definition of ICRs in part 3 of the draft Bill about communications data (Clause 47) was not the same as that in part 4 of the Bill on data retention (Clause 71(9)).[77] He said:

> "While the two provisions contain some similarities, they have significant drafting differences. At its core one is concerned with "data which may be used to identify a telecommunications service", whereas the other is concerned with "communications data which may be used to identify, or assist in identifying, the internet protocol address or other identifier of … apparatus."[78]

114. He also pointed out in evidence to the Joint Committee that "Clause 47(4) uses the terms 'internet service' and 'internet communications service'. Neither term is defined."[79]

115. Ian Batten suggested that the definition of ICRs in Clause 47(6)(b) was such that it would not include data that would be essential for ICRs to have value:

> "returning to [Clause] 47(6)(b) of the draft bill, the requirement for Internet Connection Records is that the data used should be "generated or processed by a telecommunications operator in the process of supplying the telecommunications service" But the TCP header, which I suspect is what is intended to be referred to here, is categorically not processed or generated by the telecommunications service. The telecommunications service need only look at the IP header. The IP header does not provide sufficient information to identify particular streams."[80]

116. CSPs who gave evidence said they had discussed the definition of ICRs with the Home Office but were not yet clear exactly what they would comprise. Adrian Gorham of O2 said "We are nearly there on the clarification of what makes up the record",[81] while Simon Miller of 3 said "The issue here is that we know that an internet connection record is going to be something like a simplified version of a browser history, but we do not know exactly what it is going to be."[82]

117. Mark Hughes, President of BT Security, concluded that "In the Internet connection records space, for example, it is difficult for us to comment because we are not defining the purpose for which it is intended."[83] In their written evidence, BT said "it would be helpful if Government would explain how the new types of data which fall within the ICR provisions are different from those that fall within the current regime. This will allow CSPs properly to scope capability and cost, and to identify what methods we could employ to generate ICRs."[84]

EMBARGOED until 09.00 on 11 February 2016

76 Written evidence from the Center for Democracy & Technology (IPB0110)
77 See, also, written evidence from techUK (IPB0088) and Virgin Media (IPB0160)
78 Graham Smith, Evidence to the House of Commons Science and Technology Committee, November 2015
79 Written evidence from Graham Smith (IPB0126)
80 Written evidence from Ian Batten (IPB0090)
81 Q 152 (Adrian Gorham, O2)
82 Q 152 (Simon Miller, 3)
83 Q 104 (Mark Hughes, BT Security)
84 Written evidence from BT (IPB0151)

118. The Home Office in their written evidence provided more detail on the proposed composition of ICRs.[85] This material was only available after the Committee's oral evidence sessions with CSPs had taken place.

119. The Internet Service Providers' Association provided us with helpful supplementary written evidence in light of the Home Office's written evidence and the Home Secretary's evidence on 13 January. ISPA outlined what it regarded to be a number of significant remaining areas of uncertainty over ICRs, and that the term ICR itself was "imprecise and requiring further work".[86]

120. **We acknowledge that, as with communications data, it is difficult to provide definitions broad enough to capture the variety of ways in which communications are conducted on the internet, and may be conducted in the future, while still providing sufficient clarity, technical detail and precision.**

121. **We welcome the additional information the Home Office has provided on ICRs, though we are not in a position to assess the extent to which it meets the concerns of witnesses as to a lack of clarity.**

122. ***We recommend that the definition of Internet Connection Records should be made consistent throughout the Bill and that the Government should give consideration to defining terms such as 'internet service' and 'internet communications service'. We recommend that more effort should be made to reflect not only the policy aims but also the practical realities of how the internet works on a technical level. (Recommendation 7)***

123. One issue on which many witnesses were agreed was that the Home Secretary's description of ICRs as "simply the modern equivalent of an itemised phone bill"[87] was inaccurate. Big Brother Watch said:

> "The Home Secretary has stated that this data is "*the internet equivalent of a phone bill*"; however this is not entirely accurate. A telephone bill reveals who you have been speaking to, when and for how long. Your internet activity on the other hand reveals every single thing you do online."[88]

124. Professor John Naughton and Professor David Vincent commented that:

> "the Secretary of State said that an Internet Connection Record was "simply the modern equivalent of an itemised phone bill". This is a deeply misleading analogy, because—whatever it turns out to be—an ICR in the current technological context will be significantly more complex and harder to compile than an itemised bill."[89]

125. Similar points were made by a number of other witnesses, including Dr Paul Bernal, Entanet International Limited, Graham Smith and GreenNet Limited.[90] The Home Secretary said to the Committee that:

85 Written evidence from the Home Office (IPB0146)
86 Written evidence from ISPA (IPB0164)
87 HC Deb, 4 November 2015, col 970
88 Written evidence from Big Brother Watch (IPB0007)
89 Written evidence from Professor John Naughton and Professor David Vincent (IPB0131)
90 Written evidence from Dr Paul Bernal (IPB0018), Entanet International Ltd (IPB0022), Graham Smith (IPB0126) and GreenNet Ltd (IPB0132)

EMBARGOED until 09:30 on 11 February 2016

> "It is, again, another attempt to be helpful in describing. The point of the comparison is to say that at the moment law enforcement and agencies have access to data in relation to telephony, which enables them to identify, if somebody has gone missing, with whom they have been in contact prior to going missing. As people move from telephony to communications on the internet, the use of apps and so forth, it is necessary to take that forward to be able to access similar information in relation to the use of the internet. I would say it is not inaccurate and it was a genuine attempt to try to draw out for people a comparison as to what was available to the law enforcement agencies now—why there is now a problem—because people communicate in different ways, and how that will be dealt with in the future. It is about communications from one device to another."[91]

126. **We do not believe that ICRs are the equivalent of an itemised telephone bill. However well-intentioned, this comparison is not a helpful one.**

The feasibility of ICRs

127. Irrespective of the clarity of the definition of ICRs, witnesses raised a number of issues about the technical feasibility of the proposal. The issue of costs, in relation to the generation and storage of ICRs, will be considered in the section on Data Retention (see paras 187–197).

Constant connections

128. The Committee was told that many internet communication services, such as Facebook and Twitter, communicate constantly to keep their feeds up to date. This is true of web browsing on a computer, but it is a particularly acute issue for applications on mobile and tablet devices which are likely to be on all day and potentially all night too.

129. Andrews & Arnold Ltd, a small ISP and hardware provider, said that:

> "If the mobile provider was even able to tell that [a person] had used Twitter at all (which is not as easy as it sounds), it would show that the phone had been connected to Twitter 24 hours a day, and probably Facebook as well. This is because the very nature of messaging and social media applications is that they stay connected so that they can quickly alert you to messages, calls, or amusing cat videos, without any delay."[92]

130. The conclusion of a number of witnesses was that ICRs would only tell law enforcement that the Facebook or Twitter app was active, but not whether it was being used nor for what reasons. As Dr Paul Bernal concluded, "the 'connection' event has little relationship to the use of the service ".[93]

EMBARGOED until 09:30 on 11 February 2016

91 Q 264 (Theresa May MP)
92 Written evidence from Andrews & Arnold Ltd (IPB0001)
93 Written evidence from Dr Paul Bernal (IPB0018)

Sources and destinations

131. Mobile phone providers explained to the Committee that they face some challenges in implementing the systems necessary for IP resolution, due to the way they route internet traffic to and from smartphones, but were working on developing such systems in order to comply with the requirements of the Counter Terrorism and Security Act 2015.[94]

132. The Committee were told by the IT-Political Association of Denmark that "if the smartphone connects to the internet through a WiFi access point (for example a WiFi hotspot in a hotel or pub), the ISP serving that access point only sees connections coming from the access point device itself."[95] The result would be that where a mobile user accessed the internet through public WiFi, an ICR would not identify them. The issue of whether small organisations providing WiFi to customers should potentially be required to retain data is covered in the Data Retention section (paras 210–223).

133. A similar issue exists with the use of Virtual Private Network (VPN) connections which mask the IP address of the user and with anonymisation systems such as Tor.[96] The IT-Political Association of Denmark said:

> "If the individual uses a VPN connection, the destination address in the ICR will be that of the VPN server, not the real destination of the traffic. Even if VPN providers are subjected to similar ICR retention requirements, it will only apply to UK VPN providers and not foreign ones. Another possibility is to use Tor (a well-known anonymisation network)."[97]

134. F-Secure pointed out that it may also be difficult to obtain meaningful information about the destination IP address using an ICR:

> "With Internet Connection Records, it is important to remind the Committee that the access network level logs give a poor signal to noise ratio. For instance, in the case of most of the websites, the only thing logged would be that the user's computer connected to Akamai's, Microsoft's, Amazon's or Google's cloud services. These are called Content Delivery Networks (CDNs) and they provide an added level of technology abstraction between the end user and the actual service that the user accesses."[98]

135. It was also suggested that the increasing use of encrypted communications could render ICRs redundant.[99] Andrews & Arnold said:

> "There is also an increasing trend within the industry to encrypt everything. Once confined to on-line banking, secure web sites are now being used for normal everyday business web pages. HTTPS is already extensively used by Facebook and Google and many others, and over the next few years it is likely to become quite rare for a web site to be unencrypted. At present some level of deep packet inspection can find the web site name of an encrypted web site

EMBARGOED until 09:30 on 11 February 2016

94 Q 146 (Jonathan Grayling, EE)
95 Written evidence from IT-Political Association of Denmark (IPB0103)
96 See, for example, written evidence from Brass Horn Communications (IPB0067) and The Tor Project (IPB0122)
97 Written evidence from the IT-Political Association of Denmark (IPB0103)
98 Written evidence from F-Secure Corporation (IPB0118)
99 See, for example, written evidence from the ADS Group (IPB0083)

> from the initial negotiation, but this loophole is being plugged in the more modern protocols."[100]

136. Dr Richard Clayton questioned how valuable the destination information might be, due to the way in which internet content is provided to users:

> "There is an inherent assumption here that there is a one-to-one correspondence between an ICR and an intentional visit to a website and that is not the case today and will be far less so in the future. Some modern browsers 'prefetch' data so that when you click on a link the page will be immediately available. In these circumstances, ICR will record a 'visit' to a linked website whether the link is clicked or not. Modern websites can be extremely complex with text, images and adverts being served from dozens of different servers. The ICR data will be unable to distinguish between a visit to a jihadist website and visiting a blog where, unbeknown to the visitor (and the blog owner) the 329th comment (of 917) on the current article contains an image which is served by that jihadist site. So an ICR will never be evidence of intent—it merely records that some data has flowed over the Internet and so it is seldom going to be 'evidence' rather than just 'intelligence'."[101]

137. The practical impact of this point was made to the Committee by Adrian Kennard of Andrews & Arnold Ltd:

> "I did a blog post today, and anyone who reads it will find they have accessed Pornhub because there is a tiny one-pixel image in the corner. They do not know that, but it will appear on the Internet connection record if they access my blog. That was deliberate, but there could be lots of things on websites, advertising networks and so on, that will create all sorts of misleading and confusing data even without someone trying to be misleading."[102]

Defining communication services

138. One of the proposed purposes for which an ICR may be accessed by law enforcement is to identify a communication service that they are using. Given the nature of the internet, it may not always be clear whether someone is using a service to communicate. Dr Paul Bernal said that:

> "the information gathered through ICRs would fail to capture a significant amount of the 'communications' that can and do happen on the internet—because the interactive nature of the internet now means that almost any form of website can be used for communication without that communication being the primary purpose of the website. Detailed conversations, for example, can and do happen on the comments sections of newspaper websites: if an analysis of ICRs showed access to www.telegraph.co.uk would the immediate thought be that communications are going on?"[103]

EMBARGOED until 09:30 on 11 February 2016

100 Written evidence from Andrews & Arnold Ltd (IPB0001)
101 Written evidence from Dr Richard Clayton (IPB0085)
102 Q 123 (Adrian Kennard)
103 Written evidence from Dr Paul Bernal (IPB0018)

The processing required to create and store ICRs may be too burdensome

139. A number of witnesses suggested that Deep Packet Inspection (DPI) would be required to create ICRs and that this would create a considerable processing and cost burden for CSPs. The IT-Political Association of Denmark said that: "some form of DPI will be required if ICRs include server names, and this will substantially increase the cost of data retention. With the increasing use of encryption for web traffic (HTTPS), it may even be impossible to determine the server name with DPI."[104]

140. Gareth Kitchen told the Committee that:

> "It has also become clear that the CSPs would have to upgrade their networks to enable them to capture communications data utilising Deep Packet Inspection technologies to fulfil the requirements of creating and storing these Internet Connection Records … These Internet connection records can only be 'manufactured' at the CSP as a by-product of interception using deep packet inspection technologies."[105]

141. Daniel Walrond said that "the amount of data the Bill is requiring ISPs to store in the form of Internet Connection Records is staggering. The specialized network equipment required to capture the data, and the data storage required is completely out of line with the turnover of a small ISP."[106]

142. The Committee were told that this would be possible by Mark Hughes, President of BT Security, although the cost—particularly of storing the data—would be substantial.

> "Technically, it is feasible to separate various parts of the packets; we can deploy tools to do that … The capital investment—the deep packet inspection-type equipment that needs to be put in place—has to be factored against the very strong growth, or fast growth, in bandwidth over the period … it is skewed quite heavily towards making sure that there is storage. It is not to say that the initial investment is not insignificant, but the storage is also a significant part of it."[107]

The challenges encountered by the Danish system

143. Many witnesses pointed to the experience of Denmark, which previously operated a similar system to ICRs but had subsequently cancelled the project.[108] The Danish system encountered a number of practical problems, many of which have been discussed in the section above.

EMBARGOED until 09:30 on 11 February 2016

104 Written evidence from the IT-Political Association of Denmark (IPB0103)
105 Written evidence from Gareth Kitchen (IPB0059)
106 Written evidence from Daniel Walrond (IPB0065)
107 Q 102, 109 (Mark Hughes, BT Security)
108 See, for example, Q 64, 74 (David Anderson QC), Q 212 (Eric King), and written evidence from Andrews & Arnold Ltd (IPB0001), Big Brother Watch (IPB0007), Dr Paul Bernal (IPB0018), Simon Pooley (IPB0060), Daniel Walrond (IPB0065), techUK (IPB0088), Ian Batten (IPB0090), Digital-Trust CIC (IPB0117) and Privacy International (IPB0120)

Box 2: Session logging in Denmark

The Danish system of session logging internet traffic required ISPs to retain the source and destination IP addresses and port numbers, the transmission protocol and timestamps. ISPs could choose to retain the first and last packet of a session or to conduct "sampling" by retaining every 500th packet at the boundaries of their network. Most ISPs chose this latter option.

The system did not require the retention of domain names and did not involve Deep Packet Inspection.

An evaluation by the Danish Ministry of Justice in December 2012 identified challenges for the police in handling the amount of data and technical shortcomings, such as an inability to identify individual customers when Carrier-Grade Network Address Translation was in use. The result was that communications data from session logging has only been used in a limited number of cases and the system was repealed in June 2014.

The Ministry of Justice has indicated that session logging could be re-introduced if the technical problems can be properly addressed.

Source: The IT-Political Association of Denmark[109]

144. There were a number of differences between the Danish system and the proposed ICRs, not least because of compromises in the design of the approach taken. Jesper Lund, of the IT-Political Association of Denmark said:

> "The main compromise in Denmark was that communications service providers were allowed to retain internet connection records at the boundary of their network, which is normally not a problem. It was not seen as a problem in 2005 because at that time the sharing of IP addresses was fairly limited. But since we have had more devices using the internet, especially smart phones and tablets which need lots of IP addresses, we have sharing of IP addresses and when the connection is done at the boundary of the network it is sometimes impossible to distinguish between different customers. That was certainly a limitation and was a factor in the limited effect of the Danish system. I should also point out that it affects only roughly half of the customers who were subject to internet connection record retention."[110]

145. The Home Secretary told the Committee that:

> "we have been talking to the Danes about their experience. There are a number of ways in which it is different. One of them is in relation to how information is due to be collected. I would best describe it—as it was described to me—that part of this is about at what point on the network you are accessing the information. We will be accessing it at a different point from the point at which the Danes were accessing it. They were getting a lot of peripheral information that did not enable them to link accounts to users, as I understand it. Another element is what we have already done in relation to IP address

109 Written evidence from the IT-Political Association of Denmark (IPB0103) and QQ 235–238, 243, 247–249 (Jesper Lund, IT-Political Association of Denmark)

110 Q 237 (Jesper Lund, IT-Political Association of Denmark)

EMBARGOED until 09:30 on 11 February 2016

> resolution through the Counter-Terrorism and Security Act. When you put these together, it gives us that greater capability.
>
> There are some other differences in relation to costs, for example, in the Danish system. As I understand it, the costs were borne largely by the CSPs. We have an arrangement for providing for cost recovery here in the UK. There are a number of differences, but, in talking about the point at the network, it is trying to do it in a simplified way, which shows that there is a technical difference in the way we are doing it."[111]

146. **The Committee acknowledges that there are important differences between the ICR proposal in the draft Bill and the system which was used in Denmark. We believe that the Home Office has learned lessons from the Danish model that will increase the chances of ICRs being effective.**

147. ***We recommend that the Government should publish a full assessment of the differences between the ICR proposal and the Danish system alongside the Bill. (Recommendation 8)***

ICRs could work

148. Other witnesses were more confident that ICRs were a feasible option. The BCS, The Chartered Institute for IT said that:

> "The requirements are feasible but only with the active participation and co-operation of the ISP at a cost which is ultimately recovered from the ISP's customers. The imposition of a retention order on an ISP is likely to require the reconfiguration of their network and the generation and storage of additional data to comply with the order."[112]

149. Virgin Media said that "We believe retention of Internet Connection Records ('ICRs') may be technically feasible but is likely to be complex and costly."[113]

150. **The Committee is grateful to the many witnesses who submitted detailed consideration of Internet Connection Records. We urge the Government to explain in its response to this report how the issues which have been raised about the technical feasibility of ICRs will be addressed in practice.**

The purposes for which ICRs can be used

151. The Home Office said that ICRs will serve three purposes supporting law enforcement investigations:

> "1. To assist in identifying who has sent a known communication online, which often involves a process referred to as internet protocol (IP) address resolution.
>
> 2. To establish what services are being used by a known suspect or victim to communicate online, enabling further CD requests to be made to the providers

111 Q 265 (Theresa May MP)
112 Written evidence from BCS, The Chartered Institute for IT (IPB0075)
113 Written evidence from Virgin Media (IPB0160)

EMBARGOED until 09.30 on 11 February 2016

of those online services e.g. to establish who the suspect or victim has been communicating with.

3. To establish whether a suspect has accessed illegal services online e.g. to access illegal terrorist material or for the purposes of sharing indecent imagery of children." [114]

152. These are set out in the Bill in Clause 47 (4).

153. Keith Bristow, Director General of National Crime Agency, told the Committee that:

> "We cannot request data retained on internet connection records unless it is for the specific purposes … If there is a vulnerable missing person—a young person perhaps—and we are concerned about what arrangements they may have put in place to go abroad or to travel, we could not request access to an internet connection record to give us the lead to pursue that point."[115]

154. Assistant Chief Constable Richard Berry of the National Police Chiefs' Council, added:

> "There are other policing purposes that we would require access to internet connection records for … for example; a banking website or, indeed, a travel website … In a particular case in relation to human trafficking that involves booking flights and the movement of people, we would not be able to obtain that data under the provisions of this Bill. Perhaps I can speak from personal experience having run a large-scale anti-human trafficking operation where 85% of the actionable intelligence came from communications data. That was in the mobile phone era of 2008. We certainly could not repeat that kind of activity now, because the mobile internet communications platforms are where most people now communicate and do those transactions."[116]

155. **We agree that all of the proposed purposes for which access to ICRs could be sought are appropriate. Furthermore, *we recommend that the purposes for which law enforcement may seek to access ICRs should be expanded to include information about websites that have been accessed that are not related to communications services nor contain illegal material, provided that this is necessary and proportionate for a specific investigation. (Recommendation 9)***

156. A related issue on the purposes for which communications data more generally may be sought by law enforcement is considered in paras 84–88.

Data Retention

157. Part 4 of the Bill provides the Secretary of State with a power to require Communication Service Providers to retain communications data, when it is proportionate and necessary, for a range of specified purposes for a maximum period of 12 months. This power will replace the data retention requirements currently set out in Data Retention and Investigatory Powers Act 2014 and the Counter Terrorism and Security Act 2015. This

114 Home Office, *Operational Case for the Retention of Internet Connection Records*, 4 November 2015
115 Q 26 (Keith Bristow)
116 Q 26 (Richard Berry)

EMBARGOED until 09:30 on 11 February 2016

will provide law enforcement with a degree of confidence that the relevant data will be available even when the CSP no longer has a need to process it for their own purposes.

158. Although not new, this was one of the more controversial parts of the Bill, and a number of witnesses were critical of its inclusion. The Center for Democracy and Technology told the Committee that:

> "legislation providing for data retention notices that could potentially require the retention of the communications data of every individual in the UK is manifestly incompatible with the rights to privacy and the protection of personal data, as found in the Charter of Fundamental Rights of the European Union ('the Charter') and applied by the CJEU in its *Digital Rights Ireland* judgment."[117]

159. Paul Lincoln of the Home Office has explained that:

> "The Government responded to the *Digital Rights Ireland* case by passing some fast-track legislation in 2014, the Data Retention and Investigatory Powers Act, which took account of the ruling on *Digital Rights Ireland*. However, on the back of that, a judicial review was brought against those powers, which Parliament had voted for. That judicial review, in the Divisional Court, found two reasons for which the powers were incompatible with European legislation. Since then, a Court of Appeal ruling has said provisionally that it did not think that *Digital Rights Ireland* set out a minimum set of standards for Governments to comply with, and on the back of that the Court of Appeal has remitted this to the court in the European Union. Therefore, we have considered that position and the powers and the associated processes for which Parliament voted in 2014."[118]

160. Not all witnesses were so confident that this part of the Bill complies with European Law. Eric King commented that:

> "my position at the moment is that we should not be legislating at all in this area until cases that are going up to the CJEU are resolved, for fear of us all wasting quite a lot of our time and having to re-amend and re-adapt the law, particularly given that we could be waiting to see how the [CTSA 2015] is implemented. I think we should hold back in this area and not include it in the Bill at all."[119]

161. David Anderson QC, Independent Reviewer of Terrorism Legislation, said that:

> "my understanding is that around five constitutional courts and some other courts, in countries such as the Netherlands, Belgium, Slovenia and Austria, have already decided that national laws based on the data retention directive, as ours was, are not valid. The High Court here said the same thing. The Swedes were made of sterner stuff; they asked Luxembourg the question, and so did our Court of Appeal. Trying to predict the results of litigation is a mug's game and I am not going to succumb to the temptation."[120]

EMBARGOED until 09:30 on 11 February 2016

117 Written evidence from the Center for Democracy & Technology (IPB0110)
118 Q 2 (Paul Lincoln, Home Office)
119 Q 212 (Eric King)
120 Q 72 (David Anderson QC)

162. **While judgements from the European Court of Justice are outstanding, legislation in this area will remain subject to potential change. Whether ICRs are included or not, we believe that, in light of the ongoing need for communications data (see paras 49–58) and the imminent expiry of DRIPA, a continued policy of some form of data retention is appropriate and that these provisions should accordingly form part of the Bill.**

Security of retained data and privacy risks

163. Clause 74 requires that the data retained must be kept securely and, once the retention period expires, deleted in a way that ensures access is impossible.

164. Many witnesses were concerned about the security risks that accompanied retaining such large datasets. Andrews & Arnold told the Committee that the:

> "retention of details of every web site visited reveals much more about a person. It can be used to profile them and identify preferences, political views, sexual orientation, spending habits, and much more. It is also useful to criminals as it would easily confirm the bank used, and the time people leave the house, and so on. This is plainly sensitive personal information, and it is clearly a huge invasion of privacy to collect and retain this information on innocent people. It is also a valuable target for criminals and so a risk for operators to retain this data."[121]

165. JISC pointed out that:

> "retaining extra communications data will increase the impact of security breaches as well as creating a more attractive target for fraudsters and other hackers; systems to facilitate law enforcement access to communications may be discovered and exploited by criminals, as lawful intercept systems on mobile phone networks and master keys for luggage have been in the past."[122]

166. Big Brother Watch felt that there was a "Lack of detail in the draft Bill regarding the security of the data and how it will be held is a concern, particularly as cyber hacking and cyber security is a growing problem for all of us. In 2014 90% of large firms and 74% of small firms in the UK suffered a security breach."[123]

167. Similar concerns were expressed by a number of witnesses, including Eris Industries, Dr Paul Bernal, Mr Ray Corrigan, Dr Glyn Moody, Mozilla, the Tor Project, and the Law Society of Scotland.[124]

168. Professor Michael Clarke, former Director of RUSI, told the Committee that "bulk data is a fact of life".[125] He said:

> "there is a sense out there that only Governments do it, but of course everybody does it. It is part of our digital society. The old phrase is that unless you are

121 Written evidence from Andrews & Arnold Ltd (IPB0001)
122 Written evidence from JISC (IPB0019)
123 Written evidence from Big Brother Watch (IPB0007)
124 See, for example, written evidence from Adrian Wilkins (IPB0003), Eris Industries (IPB0011), Dr Paul Bernal (IPB0018), Giuseppe Sollazzo (IPB0032), Mr Ray Corrigan (IPB0053), Dr Glyn Moody (IPB0057), Mozilla (IPB0099), the Chartered Institute of Library and Information Professionals (IPB0104), Open Rights Group (IPB0108), Center for Democracy & Technology (IPB0110), the Tor Project (IPB0122) and Law Society of Scotland (IPB0128)
125 Q 66 (Professor Michael Clarke)

EMBARGOED until 09:30 on 11 February 2016

> one of a very small group of people indeed, Tesco already knows a great deal more about you than MI5 ever will. Data analytics are used by everybody: by retailers, by charities like my own. Everybody uses data analytics. Bulk exploitation of data is part of our society."[126]

169. The view of CSPs who gave evidence was that the security of such data was important and challenging, but feasible. Hugh Woolford, Director of Operations, Virgin Media explained that:

> "We will obviously look to work with the government security advisers to ensure that any processes and systems that we put in place to meet this Bill would meet those requirements and then regular auditing of them. That is the best way we think we could assure that everything was secure and in place. As a matter of course, you have to create a culture and a process around it that brings rigour."[127]

170. Mark Hughes, President, BT Security explained that:

> "It is about creating a layered approach to defence, ensuring that the controls are proportionate, given the sensitivity of the data. We are talking about collecting data for the first time—data we have not collected before—and the key is to ensure that our customers and their rights are protected. That data has to be looked after very carefully, so we have to have a commensurate security wrap around them that takes account of our customers' human rights and indeed their privacy as well so that we ensure that we maintain and safeguard that."[128]

171. Adam Kinsley Director of Policy and Public Affairs, Sky, commented that: "We currently work with the Government on standards, but it could benefit from being more joined up on the Government's side. The Home Office, the ICO and the National Technical Assistance Centre having a single set of standards that we could build to would make a lot of sense."[129]

172. Richard Alcock of the Home Office assured us that: "The retention systems are built to stringent standards, and those standards are set by the Home Office. Systems do not go live unless they have been independently tested and accredited. We are very confident in the arrangements that we have to maintain security of the data retention systems, and I cannot say more than that. We completely understand the threat, and because of that we put a lot of effort into ensuring that integrity."[130]

173. The Home Office also assured us that the requirements it will place on operators will work technically. Richard Alcock has explained that:

> "We have ongoing discussions with a number of comms service providers, as I mentioned before. Those service-provider systems are constantly changing. We have a good relationship with the service providers on which we are likely to serve notice, and we have a good understanding of their current technical

EMBARGOED until 09:30 on 11 February 2016

126 *Ibid.*
127 Q 110 (Hugh Woolford, Virgin Media)
128 Q 110 (Mark Hughes, BT Security)
129 Q 110 (Adam Kinsley, Sky)
130 Q 22 (Richard Alcock, Home Office)

> systems. During all the conversations that we have with them, at no point have they said that it is impossible to implement."[131]

174. **The security of retained data, especially such potentially intrusive data, is of great importance. We have received assurances from the Home Office that it is possible to hold such data securely if high standards are set, observed, and regularly scrutinised but data theft remains an ongoing challenge.**

175. ***We urge the Government to consider the suggestion to work with the Information Commissioner's Office, the National Technical Assistance Centre and the Communications-Electronics Security Group at GHCQ, which has recognised expertise in this area, to draw up a set of standards for CSPs. (Recommendation 10)***

Retention period

176. The draft Bill allows for data retention notices to require data to be held for up to 12 months. This is the same period that currently operates under DRIPA and CTSA.

177. Christopher Graham, the Information Commissioner, said that there was insufficient justification for this 12 month period:

> "When I say that little justification has been advanced, I mean that those who are putting forward this Bill are not explaining what 12 months is about—why 12 months? If you are going to say, "We reserve the right to invade your privacy, and by the way this material has to be retained for 12 months", you have to make the case for that. Nowhere in the Bill or supporting memoranda have I seen the argument for 12 months. It is not for me to say that I think 12 months is wrong or right or that some other figure is appropriate because I am not the one seeking the powers; I am not the one who knows what we want to do with the information; I am not the one who knows how the information has been used. I am realistic; I understand that there has to be some care with which the facts are bruited abroad but nevertheless, nowhere in this 296-page package is the case actually made for 12 months."[132]

178. Paul Lincoln of the Home Office has explained that:

> "the UK decided to adopt a maximum of 12 months when it first introduced its legislation in this area. The 12 months was considered to be the right balance as to the level of intrusiveness in holding that amount of data. It was done on the basis of surveys by looking into the way in which law enforcement used the powers.
>
> The critical reason for going up to 12 months is child sexual exploitation cases. Certainly when a survey was done on this in 2012, 49% of all requests made in child sexual exploitation cases were for data between 10 and 12 months old. That is a very significant period, which is reflected in the position that we have taken."[133]

131 Q 21 (Richard Alcock, Home Office)
132 Q 227 (Christopher Graham, Information Commissioner)
133 Q 19 (Paul Lincoln, Home Office)

EMBARGOED until 09:30 on 11 February 2016

179. Chris Farrimond Deputy Director Intelligence Collection, National Crime Agency explained that:

> "in a 2012 survey right across policing in the UK, of all crime types within 0 to six months approximately 84% of comms data was applicable: that is to say, when we needed it, 84% fell within the 0 to six months, 13% within the seven to 12 months, and 3% in the 12 months-plus. But that does not give the whole picture. For child abuse, only 42% fell within the 0 to six months, and 52% fell within the seven to 12 months. There are also figures for terrorism offences, sexual offences and financial offences. We can give those figures, but this quite clearly shows that the closer you are to the date, generally speaking as soon as the investigators get hold of the case they are going to want to get the data, but sometimes it takes a bit longer, for whatever reason. For instance, we do not immediately get the referrals that I spoke about a few minutes ago involving child sexual exploitation; sometimes it can take a few months for them to come through, which may be the reason for the 52%. Either way, I think it shows pretty consistently that 12 months is a reasonable point at which to draw the line."[134]

180. Simon York, Director of the Fraud Investigation Service, HMRC, commented that:

> "the position for HMRC is a little different. Our figures show that more than 50% falls into the six to 12 month period. Indeed, quite a lot falls beyond 12 months. We are doing a lot of reactive, or historical, analysis. We have some real-time stuff, perhaps smuggling, but if it is more in the tax evasion area it can be a lot more historical; if it involves the use tax returns, we will not even do that analysis until 12 months after the year ends. We are in quite a different position from that of the National Crime Agency. Overall, we feel that 12 months is a reasonable balance to be struck, but we have a lot of cases that fall within that six to 12 month period."[135]

181. In written evidence, law enforcement representatives provided additional material to support the 12 month data retention requirement.[136]

182. Some witnesses suggested alternative models for data retention. Dr Julian Huppert has suggested: "the Committee should consider recommending a reduction in the 12 month retention period, possibly associated with data preservation orders where there is suspicion that particular data may be needed later."[137] A similar point was made by Caroline Wilson Palow, Legal Officer at Privacy International, who explained that: "The US, for instance, does not have a data retention provision, yet it is still able to solve crimes. In fact, it uses mechanisms like data preservation orders, which are much more targeted, are not across the board and can be quite effective."[138]

183. **We are not convinced that targeted retention orders are a viable alternative to a data retention provision, as they do not provide retrospective information and would be of limited value in instances where criminal action had ceased.**

134 Q 32 (Chris Farrimond, National Crime Agency)
135 Q 32 (Simon York, HMRC)
136 Written evidence from law enforcement (IPB0140)
137 Written evidence from Dr Julian Huppert (IPB0130)
138 Q 128 (Caroline Wilson Palow, Privacy International)

EMBARGOED until 09:30 on 11 February 2016

184. Some witnesses pointed to other countries, which did not use or had ceased to use data retention. Jim Killock Executive Director, Open Rights Group, said that:

> "on data retention in general, we have had a ratcheting back of data retention in a lot of Europe. These apparently essential tools have not been operational for a long time in Germany, the Czech Republic, Slovakia and a number of other places. There are about six or seven countries where these sorts of programmes have essentially been cancelled. There has not been a concomitant outcry from the police that they are no longer able to solve crimes and that there is spiralling dysfunction in the police. That has not occurred. Something to bear in mind is that there are often several routes to solving crimes. Data, through data retention or collection, is only one."[139]

185. Privacy International made a similar point in their evidence.[140]

186. **Any fixed retention period will always risk being arbitrary. We believe on balance that law enforcement have made the case for a 12 month retention period and support its inclusion in the Bill.**

Costs

187. The issue of the costs of data retention (and ICRs) was raised with the Committee by a number of witnesses.

188. The evidence from CSPs was unanimous that the full costs of the implementation of data retention and ICRs should be met by the Government.[141] TalkTalk said:

> "Retaining this data, and storing it securely, represents a significant new cost for CSPs. Whilst the Government has indicated that it accepts the principle of cost recovery (i.e. that the Government reimburses CSPs for costs associated with the data retention requirements in the Bill), these arrangements should be more explicitly outlined in the Bill to provide taxpayers and CSPs with greater clarity about how the cost recovery model will work. Without an effective and clearly defined cost recovery model, consumers face the very real risk of seeing their bills rise to pay for the implementation of the Bill."[142]

189. Jonathan Grayling of EE said:

> "We believe that the Bill should make it explicit that a company impacted by this legislation is fully able to recover the costs incurred. We believe that if there is no cap on costs based on a proportionality aspect, and the obligation and the financial impact is simply passed on to the CSP, this could result in delivering disproportionate solutions. If there is a cost recovery model that places a cap on cost and is based upon proportionality, that provides a far safer investment for taxpayers' money and the privacy of our customers."[143]

139 Q 128 (Jim Killock, Open Rights Group)
140 Q 128 (Caroline Wilson Palow, Privacy International)
141 See, for example, Q 106 (Mark Hughes, BT Security), and written evidence from Andrews & Arnold Ltd (IPB0001), Entanet International Ltd (IPB0022), Vodafone (IPB0127), GreenNet Ltd (IPB0132), EE (IPB0139), BT (IPB0151) and Virgin Media (IPB0160)
142 Written evidence from TalkTalk (IPB0154)
143 Q 152 (Jonathan Grayling, EE)

EMBARGOED until 09:30 on 11 February 2016

190. ISPA likewise said: "The final Act should enshrine full cost recovery for providers. The cost recovery provision ensures that providers are not commercially disadvantaged and acts as an important safeguard as it provides for a clear link between public expenditure and the exercise of investigatory powers."[144]

191. Mark Hughes, of Vodafone, told us that he had been told that there would be full cost recovery:

> "The Home Office has always had a policy of 100% cost recovery. They have assured us that this will continue. This is not an area that we make any money out of. We provide the very best service that we can to assist law enforcement."[145]

192. As to what those costs would be, CSPs said that it was difficult to make an assessment as they were not yet certain of what data they would need to retain.[146] Mark Hughes of Vodafone said that "Until we have been served with a notice, I would be purely speculating as to the cost. I would be uncomfortable giving you any kind of idea until the Home Office has served us with a notice. It would be significant, it is fair to say."[147]

193. Hugh Woolford of Virgin Media said:

> "I would love to give you an exact figure. We are not saying it cannot be done. Anything can be done in this space with enough time and money. We have a broad set of requirements, but to enable us to move forward we need to bring some more specificity to those so that we can start giving more accurate estimations of costs and time. Depending on how much you are trying to capture and across what frequency, one big piece of it is how much of whatever the equipment is you might need to deploy; therefore, you need to find space, power and places to host it all. It is no mean feat."[148]

194. Richard Alcock of the Home Office said that:

> "It is £174 million over a 10-year period in relation to internet connection records. Right now, under existing legislation, in the last financial year we spent around £19 million on data retention, so broadly speaking we are doubling the cost of data retention … We have worked with industry over summer to look at the likely data volumes and the costs associated with that volumetric growth over time, so even though I gave the example of £17 million a year, the reality is that the cost may go up over that time. But, as I say, we have been working very closely with the comms service providers on which we are likely to serve notice to underpin the facts and figures within the impact assessment."[149]

195. **We are not able to make an assessment of the accuracy of the data retention costs provided by the Government. We urge the Government to continue working with CSPs to improve the detail of the cost estimates for data retention to show how it will be deliverable in practice and deliver value for money.**

EMBARGOED until 09:00 on 11 February 2016

144 Written evidence from ISPA (IPB0137)
145 Q 157 (Mark Hughes, Vodafone)
146 See, for example, Q 117 (Adrian Kennard, Andrews & Arnold Ltd) and Q 147 (Jonathan Grayling, EE)
147 Q 147 (Mark Hughes, Vodafone)
148 Q 106 (Hugh Woolford, Virgin Media)
149 Q 19 (Richard Alcock, Home Office)

196. ***As the communications data will be held for purposes that are not related to the CSP's own business purposes, we agree that the Government should provide CSPs with whatever technical and financial support is necessary to safeguard the security of the retained data. While we do not agree that 100% cost recovery should be on the face of the Bill, we do recommend that CSPs should be able to appeal to the Technical Advisory Board on the issue of reasonable costs. (Recommendation 11)***

197. ***Our view is that the Government should provide statutory guidance on the cost recovery models, and that particular consideration should be given to how the Government will support smaller providers served with data retention notices. (Recommendation 12)***

Third party data

198. Many witnesses were concerned that CSPs would be required to retain "third party data" under the terms of the draft Bill. Third party data refers to data passing over a CSPs network which neither originates nor terminates there.

199. Mobile CSPs were particularly concerned that they should not be obliged to retain communications data relating to third party "over the top" Internet communications services. Vodafone explained their position against such a provision:

> "Vodafone believes the responsibility to obtain and retain this data should be held by the provider of such a service—for example Facebook, Google Mail or WhatsApp—and not by the underlying network operator including Vodafone.
>
> Network operators simply act as the "postman" for these services. If network operators were required to obtain and retain data, this would mean installing a complex new array of technology, requiring us to build systems to capture data for which we have no business purpose. We have expertise of the data which we generate in the course of running our own services for our day-to-day business activities, but we have very little knowledge, or reason to know, how any given Internet communications service or OTT service might structure its communications. The potential for this system to be ineffective, inefficient and retain too much or indeed too little data is substantial … Even if an operational case has been made, we consider that any duty to retain communications data should be imposed only on the provider of the service in question: the company which provides the service should retain the data."[150]

200. The Home Office made clear that CSPs would not be required to retain third party data.[151] Speaking in the House of Commons on 4 November 2015, the Home Secretary said: "Let me be clear: the draft Bill we are publishing today is not a return to the draft Communications Data Bill of 2012. It will not include powers to force UK companies to capture and retain third party internet traffic from companies based overseas."[152]

201. CSPs and others said that the framing of the draft Bill still left them open to retaining third party data. LINX told the Committee that:

150 Written evidence from Vodafone (IPB0127)
151 Written evidence from the Home Office (IPB0146)
152 HC Deb, 4 November 2015, col 969

EMBARGOED until 09:30 on 11 February 2016

> "We are concerned that, contrary to direct assurances the Home Secretary gave to Parliament, the terms of this Draft Bill would authorise the Secretary of State to impose requirements on Internet access providers (ISPs) to collect third party data."[153]

202. EE said that "The Home Office has provided verbal assurance that there will be no requirement for EE to retain third party data. However, on the face of Bill there is very little limitation on what Government could require telecommunications operators to do."[154]

203. TalkTalk agreed, saying:

> "TalkTalk welcomes the exclusion of third party data requirements. The draft Bill, however, would benefit from greater clarity on this point. Clause 71(9) should be modified to make clear that 'relevant communications data' exclusively relates to data generated on a CSP's own network, or data processed by that operator in order to provide a service. This would distinguish it from transit data that may use a CSP network, but is of no relevance to a CSP."[155]

204. EE suggested a similar amendment in their evidence to the Committee.[156]

205. ***We agree with the Government's intention not to require CSPs to retain third party data. The Bill should be amended to make that clear, either by defining or removing the term "relevant communications data". (Recommendation 13)***

206. There were concerns too that CSPs would be required not just to retain data but to generate new data. ISPA said that:

> "The Bill goes beyond the current legal framework in that providers will no longer only be required to retain data that is or will be generated for business purposes. Clause 71(8)(b) refers to "collection, generation or otherwise" which suggests that providers may be required to specifically generate data, i.e. it may require providers to change their business operations or make changes to their business model."[157]

207. EE said "The power to require a provider to "generate" data for the purposes of retention ([Clause] 71(8) (b)) is also of concern (one that also existed with the Draft Communications Data Bill), with fears that it could be used to require a provider to generate data that does not relate to providing a service to our customers. Again, a modification of Clause 71(9) as above would preclude this requirement."[158]

208. Similar comments were made by Andrews & Arnold Ltd and techUK.[159]

209. ***We recommend that the Government should clarify the types of data it expects CSPs to generate and in what quantities so that this information can be considered when the Bill is introduced. (Recommendation 14)***

153 Written evidence from LINX (IPB0097)
154 Written evidence from EE (IPB0139)
155 Written evidence from TalkTalk (IPB0154)
156 Written evidence from EE (IPB0139)
157 Written evidence from ISPA (IPB0137)
158 Written evidence from EE (IPB0139)
159 Written evidence from Andrews & Arnold Ltd (IPB0001) and techUK (IPB0088)

EMBARGOED until 09:30 on 11 February 2016

Definitions of telecommunications provider and telecommunications service

210. The Bill extends the range of providers that might receive a retention notice. JISC told the Committee that:

> "Under current law, orders to prepare for future investigations (for example by data retention or interception capabilities) can only be made against "public telecommunications operators" (see DRIPA section 1(1) and RIPA section 12(1)(a)). Private networks—such as Janet and networks within universities, colleges and businesses—can be required to disclose specific communications data they already have (RIPA section 22) or to implement targeted interception warrants (RIPA section 5). However they cannot be required to modify their activities or systems in advance so as to facilitate such activities. The new Bill applies all its powers, both preparatory and targeted, to "telecommunications operators": a term defined in Clause 193 so as to include every organisation and home with any kind of connection to a telecommunications network."[160]

211. BT also suggested that the inclusion of private networks would be problematic:

> "We are therefore concerned that Clause 189 of the IPB extends Government's power to serve a capability notice on a CSP to cover all the "telecommunications services" it provides, rather than just "public telecommunications services", as under the current regime. BT offers a significant range of services that do not fall into the "public" category. Examples include services offered under compulsion (Wholesale Line Rental or Local Loop Unbundling offered by BT Openreach) and private networks (a network provided to a large company for internal communications). This change could have significant implications for BT."[161]

212. ISPA said they were:

> "concerned about the unclear and potentially wide-ranging definition of providers and services that are covered by the Bill. The Government has stressed publicly that it has drafted the Bill in consultation with a number of operators that are likely to be served a data retention notice. It is not clear if this has been of a suitably detailed level to enable a full and clear assessment. Moreover, the powers of the Bill could easily be applied to a whole range of other providers and services whose input has not been considered, not least given the new extension to 'private' networks."[162]

213. Similar points were made by the Institute for Human Rights and Business, Mozilla, Chartered Institute of Library & Information Professionals, Open Rights Group and F-Secure.[163] There were concerns that smaller ISPs and others would face significant challenges if they were required to retain communications data.

EMBARGOED until 09:30 on 11 February 2016

160 Written evidence from JISC (IPB0019)
161 Written evidence from BT (IPB0151)
162 Written evidence from ISPA (IPB0137)
163 Written evidence from the Institute for Human Rights and Business (IPB0094), Mozilla (IPB0099), the Chartered Institute of Library & Information Professionals (IPB0104), Open Rights Group (IPB0108) and F-Secure Corporation (IPB0118)

214. As Entanet International Ltd told the Committee, "The definition of Communications Service Provider is extraordinarily wide—it could extend to a coffee shop offering free Wi-Fi."[164]

215. This was confirmed by the Home Secretary in her evidence to the Committee, who in response to a question about whether Wi-Fi in coffee shops might be included, said:

> "Yes. That is left open—and rightly so. If you look at how people are conducting their business, their interactions and their communications today, they are doing that on the move and in a whole variety of settings. It may very well be that there are circumstances where it is appropriate to have that discussion and, potentially, to ask for information to be retained. It is about having that flexibility."[165]

216. According to Andrews & Arnold:

> "It seems clear from the Home Office that they are intending to only serve notices on those larger ISPs that are already subject to notices, and with which they have already had extensive discussions. They have indicated that they are not intending to target smaller ISPs, and even if they did, that ISPs would not be expected to log and retain data for which they simply do not have such a capability, and that they would not expect any collection of "third party data" or information from "over the top services"." [166]

217. Similar points were made by the Rev Cecil Ward and Philip Virgo.[167]

218. Clause 72 requires the Secretary of State to take reasonable steps to consult with an operator before giving them retention notices, and Clause 73 enables operators to refer notices to the Technical Advisory Board and the Investigatory Powers Commissioner.

219. Richard Alcock of the Home Office has assured us that: "We make balanced judgments on the service providers on which we serve notices, and we sometimes have to make hard choices about where we put data retention notices. Obviously I cannot go into detail about the organisations that we would intend to serve notices on, but we have been working with every organisation that would be likely to have a notice served on it."[168]

220. **We believe that the definition of telecommunications service providers cannot explicitly rule out smaller providers without significantly compromising the data retention proposals as a whole. We acknowledge that the potential burden of data retention notices, particularly for smaller providers, could be acute. This makes the clarification of cost models, as we have recommended above, essential.**

221. **We are reassured that a route of appeal for data retention notices exists in Clause 73.**

EMBARGOED until 09:30 on 11 February 2016

164 Written evidence from Entanet International Ltd (IPB0022)
165 Q 269 (Theresa May MP)
166 Written evidence from Andrews & Arnold Ltd (IPB0001)
167 Written evidence from Rev Cecil Ward (IPB0013) and Philip Virgo (IPB0061)
168 Q 19 (Richard Alcock, Home Office)

222. The definitions of telecommunications service and telecommunications operator in the draft Bill also cover providers based overseas which supply services to people in the UK. Apple told the Committee that:

> "As defined in relevant EU Telecommunications Law, Apple is not an electronic communications service provider. The Investigatory Powers Bill seeks to extend definitions in this area to an extent beyond that provided for in relevant EU law. The draft bill makes explicit its reach beyond UK borders to, in effect, any service provider with a connection to UK consumers."[169]

223. The issues related to the extraterritorial effect of these provisions are considered in paras 513–518.

Retention notices

224. The Secretary of State will issue relevant CSPs with retention notices specifying what data is required to be retained for what period. Clause 77 prohibits CSPs from disclosing the existence and contents of a retention notice to any other person. This has been challenged by a number of potential recipients of retention notices.

225. Andrews & Arnold Ltd questioned the justification for this prohibition:

> "whilst I can understand operation reasons for not revealing targeted intercept warrants, a retention order does not relate to a suspect or a case, and so has no reason to be secret… If an operator wants to discuss the notice with equipment vendors, technical working groups and forums with other ISPs or even their customers they are prohibited from doing so."[170]

226. Concerns were also raised about the implications for whistle-blowers. Naomi Colvin told the Committee that "An explicit public interest defence should be included in the Bill, which would protect both whistleblowers and security researchers working in the public interest."[171] The issue of whistle-blowers is considered further later in the report (see paras 560 and 627–630).

227. In her letter to the Committee, the Home Secretary explained the provision in the draft Bill:

> "Disclosing the existence of a notice would risk undermining national security and the prevention and detection of crime. For example, criminals might start to use the services of companies that are not subject to a notice. The commercial interests of that company could be prejudiced if the Government made the fact of a notice public and significant numbers of customers transferred their business to companies who are not subject to a notice."[172]

228. ***We understand the Government's position for not allowing the fact that a data retention notice has been served to be referred to in public. We suggest that some forum or mechanism, perhaps through the Technical Advisory Board, is made available so***

169 Written evidence from Apple Inc. and Apple Distribution International (IPB0093)
170 Written evidence from Andrews & Arnold Ltd (IPB0001)
171 Written evidence from Naomi Colvin (IPB0063)
172 Written evidence from Theresa May MP (IPB0165)

EMBARGOED until 08:30 on 11 February 2016

that CSPs subject to such notices can share views on how best to comply with them. (Recommendation 15)

229. **We believe that the Intelligence and Security Committee and the Investigatory Powers Commissioner should have access to a list of CSPs served with data retention notices and that their scrutiny will be a valuable check on the appropriate use of this power. We also acknowledge that the Information Commissioner's Office will scrutinise the information security arrangements of CSPs subject to data retention notices and will therefore need to be informed of the existence and content of relevant notices.**

Request Filter

230. Clauses 51 to 53 require the Government to establish filtering arrangements to facilitate the obtaining of communications data by relevant public authorities and to assist a designated senior officer in each public authority to determine whether he or she believes the test for granting an authorisation to obtain data has been met.

231. The Home Office has said that the Request Filter would be used for complex communications data inquiries that cover several CSPs. Rather than a public authority having to submit separate requests to several CSPs, it is proposed that it would submit one request to a specialist unit run by the Home Office. This unit would operate a Request Filter that would interrogate the multiple CSP databases and automatically analyse the returns, providing investigators with only the relevant data and destroying any data once it was no longer needed.

232. The proposals are very similar to those in Clauses 14 to 16 of the Draft Communications Data Bill 2012, which also proposed a Request Filter. The key change from the earlier Bill is that the Secretary of State must now consult the Investigatory Powers Commissioner about the principles on the basis of which the Secretary of State shall establish the filter.[173] Other changes provide that the designated senior officer must consider that what is proposed must be proportionate to what is sought to be achieved[174] and that the Secretary of State may restrict the number people who are cable of acting as a designated senior officer with regard to the Request Filter.[175]

233. The Home Office said that "the filtering arrangements will minimize the interference with the right to privacy, in particular respect for personal correspondence, to which requests for internet based communications data will give rise thereby ensuring that privacy is properly protected."[176]

234. The Request Filter was broadly supported by the Information Commissioner's Office, who said:

> "If this mechanism is effective this could reduce privacy intrusion such as when trying to resolve IP addresses. However how this would work in practice would require some attention and close review by the Investigatory Powers

173 Clause 51(5)
174 Clause 52(5)
175 Clause 53(4)
176 Home Office, *Draft Investigatory Powers Bill: Explanatory Notes*, Cm 9152, November 2015, para 137

EMBARGOED until 09:30 on 11 February 2016

> Commissioner (IPC) to ensure that it is achieving its aims and not being used in inappropriate ways."[177]

235. The proposal was also welcomed by Virgin Media, though with a note of caution about the need for safeguards:

> "we understand that the intention is for a request for data to be passed through the filter to ensure that only the relevant data is passed on to law enforcement. If operated in this way it should help to protect privacy. Clarification around scope, controls, security, oversight and implementation is required either on the face of the Bill or in secondary legislation. It is not clear how exactly concerns expressed by the Joint Committee (Communications Data Bill 2012) will be addressed."[178]

236. In 2012 the Joint Committee on the Draft Communications Data Bill concluded that:

> "The Request Filter will speed up complex inquiries and will minimise collateral intrusion. These are important benefits. On the other hand the filter introduces new risks, most obviously the temptation to go on "fishing expeditions". New safeguards should be introduced to minimise these risks. In particular the IoCC should be asked to investigate and report on possible fishing expeditions and to test rigorously the necessity and proportionality of Filter requests."[179]

237. The key changes to the clauses from those in the Draft Communications Data Bill, as outlined in paragraph 232 above, seek to address those concerns. Additionally, Paul Lincoln of the Home Office has explained to us that:

> "There is oversight by the Investigatory Powers Commissioner as a starting point in terms of all the powers in the Bill, but in addition to that we have greater defence in the Bill to make sure that in extremis if you are wilfully trying to abuse the system, a criminal sanction is available. There are also administrative and other sanctions available to the Government."[180]

238. **We welcome the amendments that have been made to the Request Filter proposal. They constitute an improvement on that which was included in the Draft Communications Data Bill.**

239. Views differ as to whether the Home Office was right to argue that the Request Filter minimises collateral intrusion and thus is a tool in protecting privacy. Some witnesses see it as a threat to privacy. For example, LINX stated that:

> "We do not agree with the government's characterisation of this portion of the Draft Bill as a safeguard that minimises the intrusive nature of access to communications data by reducing the volume of data that will be released to investigating officers. We think a much more accurate characterisation would be to regard these arrangements as an enormously powerful and intrusive new

177 Written evidence from the Information Commissioner's Office (IPB0073)
178 Written evidence from Virgin Media (IPB0160)
179 Joint Committee on the Draft Communications Data Bill, *Draft Communications Data Bill* (Report of Session 2012–13, HC 479, HL Paper 79) para 126
180 Q 8 (Paul Lincoln, Home Office)

EMBARGOED until 09.30 on 11 February 2016

> investigatory tool that brings the power of Big Data analysis to law enforcement investigation on an unprecedented scale."[181]

240. Eric King argued that "it permits the same sort of data-mining at a scale that so far only our intelligence and security agencies have been undertaking, and provides that to the police, but in the name of a safeguard."[182] Entanet International told the Committee that "the complex queries such a database allows make the extent of intrusion difficult to quantify or oversee on the face of the bill."[183]

241. Similar concerns were expressed by the Open Rights Group, Dr Julian Huppert, the Internet Service Providers' Association, Mcevedys Solicitors & Attorneys Ltd and Liberty.[184]

242. Another issue that was raised was the potential security risk involved in operating the Request Filter. James Blessing, ISPA Chair and Chief Technology Officer of Keycom, told the Committee that:

> "In theory, the filter is being described as a way of restricting the information recovered. That means that an automated system must be doing the requesting of the data capture from the service provider and then presenting them to an individual. That means we have to allow third-party access to our systems, which is a potential risk. In theory, it would mean that the data was less open to fishing because you are only getting back specific results, but potentially there is a whole new construction of requests that people could start making… In some ways it is a good thing and in some ways it is a concern, because, again, the details are very limited."[185]

243. Adrian Gorham of O2 also outlined his concerns about the security aspects of the filtering arrangements:

> "A third party will take bulk data from us and analyse it for the police, to make sure the police only see the data they require. My concern there would be that that third party has exactly the same level of security that we deploy ourselves in our businesses. A number of us have international standards; I would expect that third party to have that level of security, if it has my customer data. I would expect the governance that we are putting in place to go and do audits on that third party, and I would—if I am giving them my customer data—expect to be able to go and audit them myself, to ensure that they are living up to our standards as well. We are all very used to looking after security and protecting that data, but we now, with this Bill, have a third party whom we would need to give data to, and we need to be very sure that the same level of security is deployed there as well."[186]

EMBARGOED until 09:30 on 11 February 2016

181 Written evidence from LINX (IPB0097)
182 Q 213 (Eric King)
183 Written evidence from Entanet International Ltd (IPB0022)
184 Written evidence from Open Rights Group (IPB0108), Dr Julian Huppert (IPB0130), Internet Service Providers' Association (IPB0137), McEvedys Solicitors & Attorneys Ltd (IPB0138) and Liberty (IPB0143)
185 Q 124 (James Blessing, ISPA)
186 Q 155 (Adrian Gorham, O2)

244. He was supported by Jonathan Grayling of EE: "I would like to see the filter having the same security controls as the ones CSPs are compelled to provide in relation to retained data."[187]

245. Our general views on privacy risks of large CD datasets are set out in more detail in paras 163–175. They pose very considerable reputational challenges to communication and internet service providers, law enforcement investigators and to individuals if security breaches occur.

246. **We welcome the Government's proposal to build and operate a Request Filter to reduce the amount of potentially intrusive data that is made available to applicants. We believe that the technical and security challenges involved in implementing the Request Filter can be met and would urge the Investigatory Powers Commissioner to examine and report on it to ensure that it is secure.**

247. **We acknowledge the privacy risks inherent in any system which facilitates access to large amounts of data in this manner. We believe that the requirement upon law enforcement to state the operational purpose for accessing data through the filter will provide an important safeguard that can be assessed by the Investigatory Powers Commissioner and that the oversight of the Commissioner will be sufficient to prevent the Request Filter being used for "fishing expeditions" and ensure that it is used proportionately.**

Encryption

248. Clause 189 allows the Secretary of State to impose obligations on telecommunication service providers and Clause 189 (4) (c) states that these obligations could include "the removal of electronic protection applied by a relevant operator to any communications or data".

249. Paul Lincoln of the Home Office told the Committee that this was a necessary power and that:

> "The Bill itself in effect replicates the existing legislation, which has been in place since 2000, and says in effect that we should be in a similar position to that of the real, physical world, where, as David Anderson says in his report and others have said, you do not want there to be places where people are allowed to go unpoliced and ungoverned. The same should apply in the internet world. So when you have taken the steps with regard to necessity and proportionality, you can place a requirement on companies to provide you with content in the clear."[188]

250. This position was supported by Ray McClure, who explained that "Without being able to access an unencrypted message the security forces will not be able to tell if the message is a harmless exchange of say a cooking recipe, or a set of terrorist instructions. I fear that in the name of privacy the encrypted services on the internet may lead the internet to become a safe haven for evil."[189]

187 Q 158 (Jonathan Grayling, EE)
188 Q 23 (Paul Lincoln, Home Office)
189 Written evidence from Mr Ray McClure (IPB0016)

EMBARGOED until 09:30 on 11 February 2016

251. The provision in Clause 189 on removing electronic protection was the subject of considerable concern among a great many witnesses, who said that its meaning was unclear. The Information Commissioner's Office told the Committee that:

> "The practical application of such requirement in the draft is unclear in the draft bill and the accompanying Guide to Powers and Safeguards does not provide specific details to enable the full extent of the provision to be assessed."[190]

252. Similarly, techUK said:

> "In particular it still remains unclear as to whether the obligation for service providers "relating to the removal of electronic protection", as stated in Clause 189(4)(c), has any ramifications for encryption technology applied by the user of the services, and not the service provider. If the provision does have ramification for end to end encryption, this would limit companies' ability to deploy the necessary security to safeguard their customers' privacy and security, in effect compelling companies to weaken the security of their products."[191]

253. Deep concerns were expressed that the implications of this provision would undermine encryption and therefore the security of online communications and transactions. Big Brother Watch said "any part of the draft Bill which may have implications for the strength of encryption will have severe consequences for the people and the country as well. Any approach to weaken, create backdoors or simply abandon encryption must be treated with extreme caution."[192]

254. Article 19 echoed this point and suggested that it could lead to companies being compelled to install "backdoors" into their products and services:

> "Despite the Government's assurances that the draft Bill would not include 'backdoors' and that encryption would continue to be protected, it is apparent that the vires of Clause 189(4)(c) are sufficiently broad to enable the Secretary of State to make regulations requiring operators either to remove encryption services upon request, or to reduce the effectiveness of encryption. This would fundamentally undermine the use of end-to-end encryption and therefore the security of our online communications and transactions. In practice, it is equivalent to a government 'backdoor'."[193]

255. Similar arguments were made by a large number of witnesses, including Dr Paul Bernal, Apple, Facebook, Google, Microsoft, Twitter, Yahoo, Mozilla, Human Rights Watch and Liberty.[194]

190 Written evidence from the Information Commissioner's Office (IPB0073)
191 Written evidence from techUK (IPB0088)
192 Written evidence from Big Brother Watch (IPB0007)
193 Written evidence from Article 19 (IPB0052)
194 See, for example, Q 135 (Caroline Wilson Palow, Privacy International), Q 135 (Renate Samson, Big Brother Watch) and written evidence from Dr Paul Bernal (IPB0018), Ms Susan Morgan (IPB0043), Martin Kleppmann (IPB0054), Open Intelligence (IPB0066), Mr. Bernard Keenan, Dr. Orla Lynskey and Professor Andrew Murray (IPB0071), the Information Commissioner's Office (IPB0073), Scottish PEN (IPB0076), the Global Network Initiative (IPB0080), New America's Open Technology Institute (IPB0086), techUK (IPB088), Apple Inc. and Apple Distribution International (IPB0093), Mozilla (IPB0099) Access Now (IPB0112), and Facebook Inc., Google Inc., Microsoft Corp., Twitter Inc. and Yahoo Inc. (IPB0116), F-Secure Corporation (IPB0118), Human Rights Watch (IPB0123), Dr Julian Huppert (IPB0130) and Liberty (IPB0140)

EMBARGOED until 09:30 on 11 February 2016

256. A particular issue was raised in relation to end-to-end encryption, where the service provider might have not have the capability to decrypt the contents of a communication passing across its system.[195] Erka Koivunen of F-Secure explained that:

> "Some of these providers have designed their systems specifically to employ end-to-end encryption, where the service provider is not in a position to open up the encryption. The encryption goes through the service provider's systems so that even the provider is not able to see through it. The way I am reading the Bill, it would actually ban the use of strong cryptography and strong encryption and would essentially weaken our ability to use secure online services."[196]

257. Witnesses were concerned that, despite the Secretary of State needing to take into account "the technical feasibility of complying" (Clause 190 (3) (c)), there was still the potential for technical capability notice to be served that would require encrypted systems to be compromised. Andrews & Arnold Ltd said that " it appears to effectively ban a provider from offering a service that has proper end-to-end encryption"[197] and Apple said that "Although this is not explicit in the draft bill, our understanding of the government's intention is that this would require us to remove end to end encryption if that was necessary to give effect to the warrant and considered proportionate."[198]

258. The evidence from Paul Lincoln, from the Home Office, suggested that this would be the case: "If you are providing a service to UK customers and the Secretary of State and a judicial commissioner think there is necessity and proportionality in order to be able to provide that information, those companies should be required to provide that information in the clear."[199]

259. Whilst a judicial commissioner would be involved in the authorisation of the warrant to access such material in the clear, they would not be involved in the decision to serve a technical capability notice on a CSP to ensure that encryption could be removed when circumstances required. This is considered further in Chapter 4, paras 498–502.

260. Various witnesses suggested that the provision to require the removal of electronic protection would have a negative economic impact by damaging the competitiveness of UK tech businesses or encouraging them to relocate outside the UK.[200] Adrian Wilkins said that "I have already seen examples of companies that have been put off setting up operations in the UK, just as a result of the proposed legislation"[201] and Eris Industries Ltd said that "Our position is that the draft Bill would impinge vital and legitimate business interests of our company … We have also, disappointingly, taken positive steps to relocate our base of operations out of London in the expectation that this draft Bill will eventually receive Royal Assent."[202]

EMBARGOED until 09:30 on 11 February 2016

195 See, for example, Q 209 (Professor Bill Buchanan), and written evidence from Dr Paul Bernal (IPB0018), Giuseppe Sollazzo (IPB0032), Martin Kleppmann (IPB0054), the Center for Democracy & Technology (IPB0110) and F-Secure Corporation (IPB0118)

196 Q 214 (Erka Koivunen, F-Secure Corporation)

197 Written evidence from Andrews & Arnold Ltd (IPB0001)

198 Written evidence from Apple Inc. and Apple Distribution International (IPB0093)

199 Q 23 (Paul Lincoln, Home Office)

200 See, for example, written evidence from Cryptomathic Ltd (IPB0115) and ISPA (IPB0137)

201 Written evidence from Adrian Wilkins (IPB0003)

202 Written evidence from Eris Industries Ltd (IPB0011)

261. The Home Secretary in her evidence to the Committee provided some much needed clarity to the intention of the Government in relation to encryption, saying that: "The Government do not need to know what the encryption is or to know the key to the encryption."[203]

262. She told the Committee that:

> "We are not proposing in the Bill to make any changes in relation to the issue of encryption and the legal position around that. The current legal position in respect of encryption will be repeated in the legislation of the Bill. The only difference will be that the current legal position is set out in secondary legislation and it will now be in the Bill. We say that, where we are lawfully serving a warrant on a provider so that they are required to provide certain information to the authorities, and that warrant has gone through the proper authorisation process and is entirely lawful, the company should take reasonable steps to ensure that it is able to comply with the warrant that has been served on it. That is the position today, and it will be the position tomorrow under the legislation."[204]

263. ***We agree with the intention of the Government's policy to seek access to protected communications and data when required by a warrant, while not requiring encryption keys to be compromised or backdoors installed on to systems. The drafting of the Bill should be amended to make this clear. (Recommendation 16)***

264. ***The Government still needs to make explicit on the face of the Bill that CSPs offering end-to-end encrypted communication or other un-decryptable communication services will not be expected to provide decrypted copies of those communications if it is not practicable for them to do so. We recommend that a draft Code of Practice should be published alongside the Bill for Parliament to consider. (Recommendation 17)***

Equipment interference

Overview

265. Part 5 of the draft Bill provides for law enforcement and the security and intelligence agencies to undertake targeted Equipment Interference.

266. Equipment interference (EI) is any interference with equipment, conducted for the purposes of gathering intelligence or manipulating the equipment, in order to establish control, compromise functionality or gather further intelligence. Equipment in this context could include personal computers, mobile phones and tablets and large systems owned by organisations. The shorthand "hacking" is often used for EI, although not all EI activities constitute hacking as traditionally defined.

267. Equipment interference has been carried out by the security and intelligence agencies and by law enforcement for some time but this Bill is the first in which it is explicitly recognised.

203 Q 270 (Theresa May MP)
204 *Ibid.*

EMBARGOED until 09:30 on 11 February 2016

268. **The Committee welcomes the fact that the EI techniques and powers are now properly addressed in legislation.**

269. For the security and intelligence agencies, EI is currently mandated by section 5 and section 7 of the Intelligence Services Act, 1994. Law enforcement, until relatively recently, have relied on section 93 of the Police Act 1997, "Authorisations to interference with property". This has allowed the police to plant audio and video bugs inside homes, offices, vehicles and so on. In other circumstances, section 10 of the Computer Misuse Act 1990 has also been used. Section 44 of the Serious Crime Act 2015 amended section 10 the Computer Misuse Act to allow law enforcement to undertake more intrusive EI activities. The Home Office emphasised in their evidence that the draft Bill does not provide for new powers in respect of EI.[205]

270. Chris Farrimond, Deputy Director Intelligence Collection at the National Crime Agency, said "We use [EI] for a range of purposes, ranging from pretty much every-day relatively routine activities right up to far more high end. The difficulty is that trying to describe any of those techniques in this setting probably would be inappropriate."[206]

271. The Committee was given an off-the-record presentation by the Metropolitan Police and National Crime Agency where a further explanation was given of the kinds of EI activities that are used.

272. **We are grateful for the information provided about EI on visits to the Metropolitan Police and to GCHQ, which has assisted our ability to scrutinise this power.**

273. Other witnesses were able to suggest what activities EI might encompass. Erka Koivunen from F-Secure said "The term "equipment interference" is pretty elegant. When I was learning information security at school we used "exploitation", "vulnerabilities" and "attacks" to describe the same things."[207]

274. Professor Ross Anderson told the Committee that: "It is basically hacking or the installation of malware, or what the NSA calls implants and what we call remote administration tools in a machine."[208] The NUJ suggested that equipment interference:

> "means the authorities would have control over targeted devices and access to any information stored. This information could include documents, emails, diaries, contacts, photographs, internet messaging chat logs, and the location records on mobile equipment. It would also mean having powers to access anything typed into a device, including login details/passwords, internet browsing histories, other materials and communications. Draft documents and deleted files could also be accessed. In addition, the microphone, webcam and GPS-based locator technology could be turned on and items stored could be altered or deleted."[209]

275. The Electronic Frontier Foundation gave examples of how equipment interference supported by a telecommunications provider might operate:

205 Written evidence from the Home Office (IPB0146)
206 Q 37 (Chris Farrimond, National Crime Agency)
207 Q 214 (Erka Koivunen)
208 Q 91 (Ross Anderson)
209 Written evidence from the National Union of Journalists (NUJ) (IPB0078)

EMBARGOED until 09:30 on 11 February 2016

> "In 2009, a software update was sent to all owners of Blackberry devices using the Etilsat network in the United Arab Emirates. The software required manual agreement by the end-user. If accepted, the new software transformed their mobile phone into a spying device, which, as the manufacturer of Blackberry, Research In Motion (RIM), wrote, "enabl[ed] unauthorised access to private or confidential information stored on the user's smartphone." RIM warned its own users about this software, because the update masqueraded as a legitimate upgrade to improve performance of the devices. RIM also had a strong incentive to protect its hardware's reputation as a high-security device, as Blackberry smartphones had been sold to multiple government and international financial institutions. If RIM had been discovered to be the real author of such an update, it would have destroyed its reputation as a guardian of its customers' data."[210]

The case for Equipment Interference

276. The Home Office told the Committee that in the past, interception powers were sufficient to follow targets, but that "technological advances and the spread of ubiquitous encryption—wrapping information in an impenetrable blanket from sender to receiver—is resulting in an increasing number of circumstances where interception is simply not possible or effective."[211]

277. Draft Codes of Practice on Equipment Interference were published in February and November 2015, but they were limited to the activities of the Security and Intelligence Agencies.[212] It is understood that the police are operating under the Code of Practice Covert Surveillance and Property Interference, chapter 7 of which covers property interference, which discusses equipment but makes no explicit reference to interference with computer systems.[213]

278. The Draft Code of Practice on Equipment Interference for the security and intelligence agencies identifies the following objectives:

a) obtain information from the equipment in pursuit of intelligence requirements;

b) obtain information concerning the ownership, nature and use of the equipment with a view to meeting intelligence requirements;

c) locate and examine, remove, modify or substitute equipment hardware or software which is capable of yielding information of the type described in a) and b);

d) enable and facilitate surveillance activity by means of the equipment;

> "Information" may include communications content, and communications data. [214]

EMBARGOED until 09:30 on 11 February 2016

210 Written evidence from Electronic Frontier Foundation (IPB0119)
211 Written evidence from the Home Office (IPB0146)
212 Home Office, *Equipment Interference Code of Practice, Draft for public consultation,* February 2015 and Home Office, *Equipment Interference Draft Code of Practice*, November 2015
213 Home Office, *Covert Surveillance and Property Interference: Revised Code of Practice*, 2010
214 Home Office, *Equipment Interference Draft Code of Practice*, November 2015, para 1.6

279. The Home Office Factsheet on Targeted Equipment Interference stated that "During 2013 around 20% of GCHQ's intelligence reports contained information that derived from EI operations; and MI5 has relied on EI in the overwhelming majority of high priority investigations over the past 12 months."[215]

280. The Home Office argued that:

> "It is right that mainstream policing, who are at the forefront of serious crime investigations, have the less intrusive equipment interference techniques available to support their investigations. But it is also important that the use of more specialised techniques is restricted to specialist teams—as is the case across policing now—with the most sensitive capabilities delivered by the National Crime Agency on behalf of wider policing." [216]

281. Richard Berry, Assistant Chief Constable, National Police Chiefs' Council, told the Committee that "To give a police perspective on this, we use equipment interference regularly, really for tracing vulnerable and suicidal missing persons."[217]

282. Beyond Government and law enforcement there was also support for targeted equipment interference. The BCS said there was a "credible argument" for EI and Professor John Naughton and Professor David Vincent said that there was a "reasonable case" for it.[218] The Rt Hon David Davis MP told the Committee that "individual targeted equipment interference is obviously a necessity, particularly in this day of encryption. It is one way of getting around encryption and probably the most effective."[219]

283. Dr Tom Hickman said that: "It is no doubt necessary for intelligence services to have the capability to hack into computers, telecommunications systems and smart phones, just as it is necessary for them to break and enter, burgle and bug. But such powers are extremely intrusive, potentially much more intrusive than interception of communications."[220]

The case against Equipment Interference

284. Privacy International, remarked that the operational case for EI was "weak"[221] and a number of witnesses argued that the EI power was too intrusive. Article 19 said that:

> "Equipment interference (i.e. hacking), whether carried out by a government or private actor, is perhaps the most serious form of intrusion into someone's private life, given that it involves access to private information without permission or notification. It also fundamentally breaches the integrity of the target's own security measures. Unlike search warrants where the individual would at least be notified that their home or office was being searched, hacking generally takes place without a person's knowledge. It is the equivalent of the police breaking into someone's home."[222]

EMBARGOED until 09.30 on 11 February 2016

215 Home Office, *Investigatory Powers Bill: Factsheet—Targeted Equipment Interference*, 4 November 2015, p. 1
216 Written evidence from the Home Office (IPB0146)
217 Q 37 (Richard Berry)
218 Written evidence from BCS, The Chartered Institute for IT (IPB0075); Professor John Naughton and Professor David Vincent (IPB0131)
219 Q 177 (David Davis MP)
220 Written evidence from Dr Tom Hickman (IPB0039)
221 Written evidence from Privacy International (IPB0120)
222 Written evidence from Article 19 (IPB0052)

285. These remarks were echoed by the Electronic Frontier Foundation who said that it was "an extremely intrusive power … [with] a tremendous possibility for abuse".[223] Similar points were made by Privacy International and Liberty.[224]

286. **We agree that targeted equipment interference has the potential to be very intrusive.**

287. **There is nevertheless a substantive case for the targeted equipment interference power. We believe that, subject to the appropriate authorisation process involving a Judicial Commissioner, such activities should be conducted when necessary and proportionate.**

288. ***We recommend that the Government should produce a Code of Practice on Equipment Interference to cover the activities both of the security and intelligence agencies and of law enforcement. (Recommendation 18)***

Criticism of Equipment Interference

Powers too broadly defined

289. Witnesses argued that the targeted EI power was too broad, in part because definitions of key terms involved were not sufficiently specific. Big Brother Watch told the Committee that:

> "Sub-Clause 81(3)(b) allows for the "obtaining of any information" that is "connected" with the equipment covered by the warrant. Given the way the internet works and the myriad of ways in which information and systems can now connect with each other this could potentially enable much broader action than was intended by the original warrant."[225]

290. Wendy Grossman, a freelance technology journalist, made a similar point in relation to the definition of equipment:

> "The bill proposes to allow interference with "electronic devices such as computers and smart phones". The image this phrasing creates is that of either a self-contained device that is used by one or a few individuals for long-established purposes such as email, word processing, internet browsing, and so on, or perhaps the routers, switches, and other devices that direct data traffic around the internet. This is not the reality of computers today, let alone tomorrow. Modern cars are clusters of computers on wheels—ten to 30 for an ordinary car, as many as 70 for a luxury car. The same or similar is true of other vehicles from tractors to airplanes. Computers are embedded in streetlights in Glasgow, in the smart meters UK electric companies are pledged to roll out by 2020, and in automated vacuum cleaners such as the Roomba and the Dyson 360 Eye, as well as most modern TVs and washing machines."[226]

291. The Center for Democracy & Technology concluded that:

223 Written evidence from Electronic Frontier Foundation (IPB0119)
224 Written evidence from Privacy International (IPB0120) and Liberty (IPB0143)
225 Written evidence from Big Brother Watch (IPB0007)
226 Written evidence from Wendy Grossman (IPB0068)

EMBARGOED until 09:30 on 11 February 2016

> "The definition of a 'system' should also be more clearly defined. Cl 81(2) and 82(3) & (4) note that a system is a relevant system if any communications or private information are held on or by means of the system. In the Australian context, similarly overbroad language has been interpreted as potentially including the entire Internet."[227]

292. Any definition needs to be drafted in a way that the "scope of the discretion conferred" and the "manner of its exercise" are sufficiently clear that an individual is protected from "arbitrary interference".[228] In other words, drafting should make clear exactly what the authorities can do when undertaking equipment interference. While a broad definition may assist in future-proofing it could also fall foul of the courts. **We note that, if our recommendation for post-legislative review five years after the Bill's enactment is implemented (see para 710), a tighter definition can be introduced without running the risk of law enforcement and the agencies being left behind by technological advancement.**

293. **We acknowledge both the concerns of witnesses about the breadth of the definitions and the desire of Government not to inadvertently rule out access to new types of equipment or system in the future.**

294. **We believe that the involvement of Judicial Commissioners in the authorisation process may ensure that the equipment and systems targeted by EI activities will be proportionate and considered foreseeable.**

295. ***We recommend that the Government should produce more specific definitions of key terms in relation to EI to ensure greater confidence in the proportionality of such activities and that a revised Code of Practice is made available alongside the Bill. (Recommendation 19)***

Security risks

296. A large number of witnesses were concerned about the potential security risks of undertaking EI activities.[229] Most of the evidence received discussed bulk EI and therefore our consideration of this issue is later in this report (see paras 363–374)

Incompatible with data protection legislation

297. Mr. Bernard Keenan, Dr. Orla Lynskey and Professor Andrew Murray questioned whether EI was compatible with data protection legislation. "The IP Bill provisions dealing with 'Equipment Interference' provide a more explicit legal basis for this hacking. These provisions are unlikely to comply with the data security requirement of the right to data protection."[230] The Committee is also aware of challenges mounted by Privacy

EMBARGOED until 09:30 on 11 February 2016

227 Written evidence from the Center for Democracy & Technology (IPB0110)

228 European Court of Human Rights, *Malone v United Kingdom,* (1984) 7 EHRR 14 and *Weber and Saravia v Germany,* (2008) 46 EHRR SE5

229 See, for example, written evidence from Andrews & Arnold Ltd (IPB0001), Big Brother Watch (IPB0007), Mr Ray Corrigan (IPB0053), New Americas Open Technology Institute (IPB0086), Apple Inc. and Apple Distribution International (IPB0093), LINX (IPB0097), Privacy International (IPB0120) and Dr Julian Huppert (IPB0130).

230 Written evidence from Mr. Bernard Keenan, Dr. Orla Lynskey and Professor Andrew Murray (IPB0071)

International and others in the Investigatory Powers Tribunal alleging breaches of the Data Protection Act arising from current equipment interference powers.[231]

298. ***We acknowledge the importance of data protection in relation to EI activities. We recommend that the assessments undertaken by Judicial Commissioners when authorising warrants should give consideration to data protection issues. (Recommendation 20)***

299. ***We further recommend that the Home Office should make clear in the explanatory notes to the Bill or in a Code of Practice how EI activities can be conducted within the constraints of data protection legislation. (Recommendation 21)***

Admissibility of evidence

300. Unlike intercept evidence, which is inadmissible in legal proceedings, material acquired under EI warrants will be admissible in court under the terms of Clause 103. Matthew Ryder QC told the Committee that this would be "appropriate and desirable. It is consistent with the well-established presumption, that relevant evidence should be admissible in legal proceedings."[232]

301. Some witnesses were concerned that this would lead to defence lawyers arguing that digital evidence should be excluded for unreliability.[233]

302. Privacy International said:

> "hacking involves an active interference with a computer, it raises serious evidentiary concerns. Evidence obtained via equipment interference is admissible in court. Once an agent or officer takes control of a computer by hacking it, however, they have the unfettered ability to alter or delete any information on that device. This raises the risk, in the context of a criminal prosecution, of defence accusations of evidence tampering. The IP Bill currently does not contain any provisions to address this evidentiary concern. Without such safeguards, the efficacy of the use of hacking in investigating and prosecuting crimes is very questionable."[234]

303. Law enforcement witnesses told us that they believed EI material could be safeguarded sufficiently for use in court:

> "LE also recognises the importance of preserving the evidential integrity of equipment that has been the subject of EI. This will continue under the IPB and LE will work closely with prosecutors to ensure the fairness of any prosecution."[235]

304. Detective Superintendent Paul Hudson, Head of the Metropolitan Police Service Technical Unit, told the Committee that:

EMBARGOED until 09:30 on 11 February 2016

231 Investigatory Powers Tribunal, *Privacy International vs Secretary of State for Foreign and Commonwealth Affairs and GCHQ,* (2015) IPT 14/85/CH
232 Written evidence from Matthew Ryder QC (IPB0142)
233 See, for example, written evidence from Liberty (IPB0143)
234 Written evidence from Privacy International (IPB0120)
235 Written evidence from law enforcement (IPB0140)

> "Equipment interference is a covert capability, so nothing that we do under equipment interference would cause any damage or leave any trace, otherwise it would not remain covert for very long. Again, the endgame is to collect evidence to place before a court. If we were causing damage to equipment, that would reduce the ability for the evidence to be alluded to."[236]

305. ***We agree that material acquired through targeted equipment interference warrants should be admissible in court, though we share the concerns of witnesses about the risks involved. We believe that law enforcement and the security and intelligence agencies will need detailed codes of practice and appropriate procedures to ensure that evidence is not inadvertently compromised. We urge the Government to consider how it will reconcile the understandable desire of law enforcement and the security and intelligence agencies to keep their techniques secret with the need for evidential use and disclosure regimes in legal proceedings. (Recommendation 22)***

Bulk powers

306. The draft Bill provides for three types of bulk power for the security and intelligence agencies; bulk interception, bulk acquisition of communications data and bulk equipment interference. These powers would allow for the collection of large volumes of data, including communications data and content. Further warrants are then required before it can be examined. The purpose of such examination may be to pursue more information about known suspects and their associates or to look for patterns of activity that might identify new suspects. These powers are not available to law enforcement.

307. The Home Office have said that all three of these powers are currently available to the security and intelligence agencies in existing legislation. Bulk interception is provided for under section 20 of RIPA, bulk communications data acquisition in section 94 of the Telecommunications Act 1984 and bulk equipment interference by section 5 and section 7 of the Intelligence Services Act 1994.

308. David Anderson QC, the Intelligence and Security Committee and the panel convened by RUSI all concluded that new legislation should make explicit provision for bulk powers. The Home Office claims that the provisions in the Bill provide a clear statutory framework for all of the bulk powers available to the security and intelligence agencies and introduces robust, consistent safeguards across all of those powers.[237]

309. **We commend the Home Office for making explicit provision for these bulk powers and for giving the Parliament an opportunity to debate and decide upon them.**

310. The view of the Home Office that the bulk powers are not new was contested by a number of witnesses. Matthew Ryder QC explained that:

> "There is a dispute and lots of litigation about what is or is not currently authorised under the existing legislation. My view would be that there are a large number of new powers that are not properly authorised within existing legislation. … Mass surveillance or bulk interception—whatever you want to call it … is essentially something new. I understand—I was involved in the case

236 Q 169 (Detective Superintendent Paul Hudson)

237 Home Office, *Draft Investigatory Powers Bill: Guide to Powers and Safeguards*, Cm 9152, November 2015, para 38

EMBARGOED until 09:30 on 11 February 2016

> and litigated the case in the IPT last year—that the Government say that bulk interception or bulk collection is permitted under Section 8(4) [of the European Convention on Human Rights], but there is a dispute about that. There is a case on its way to Strasbourg. It has been communicated in Strasbourg. There are many of us who would say that it was not set out very clearly, if it was permitted at all, in RIPA … Chapter 2 of Part 6 on bulk communications data acquisition. That is essentially new. In other words, the large collection of communications data in bulk is something that was not clear from any legislation before. That is essentially being regulated for the first time, under this Bill."[238]

311. Professor Sir David Omand explained how, in his view, the Government position had developed on powers in this area over recent decades:

> "The legal regime under which previous Governments operated for the past 20 years, since the 1980s, was what I would describe as legal compliance; in other words, if it could be done lawfully under existing powers that Parliament had passed, Ministers would authorise such activity, after due legal advice, regardless of party—this is not a party political matter—in the interests of national security, the prevention and detection of serious crime, and economic well-being arising from causes outside the United Kingdom. That was the regime.
>
> It was really when the Investigatory Powers Tribunal took the case and reported that the Government's activity, in particular GCHQ, might be regarded as lawful under the individual statutes but failed the rule of law test because it was not clear, as your question implies, to the public … Or to Parliament. This Government have taken that to heart, and the Bill is in part the result. We have moved into a new era and I am personally very glad of that.
>
> A lot of trouble would have been saved if, say, even five years ago the codes of practice—it would not necessarily have taken new legislation—on equipment interference, investigative powers and so on had all been updated to the modern digital world. For one reason or another that was not done. The shock of discovering what was happening, for very good reason—to defend the public and our security—was all the greater. I think the lesson has been learnt."[239]

The clarity of bulk powers

312. A number of witnesses were concerned about the lack of detail as to the scope of bulk powers. Dr Paul Bernal said that "At the moment quite what these bulk powers consist of—and how 'bulky' they are—is largely a matter of speculation, and while that speculation continues, so does legal uncertainty."[240]

313. The UN Special Rapporteurs said that "the provisions on bulk interception warrants are vague and not tied to specified offences, and include ambiguous terms such as "economic well-being", heightening the risk of excessive and disproportionate interception."[241] The

238 Q 186 (Matthew Ryder QC)
239 Q 76 (Professor Sir David Omand)
240 Written evidence from Dr Paul Bernal (IPB0018) and Q 76 (Dr Paul Bernal)
241 Written evidence from the UN Special Rapporteurs (IPB0102)

EMBARGOED until 09:30 on 11 February 2016

issue of the definition of "economic well-being is considered in Chapter 6 (see paras 692–696).

314. Article 19 suggested that:

> "it is open to the Secretary of State to issue bulk warrants to obtain potentially billions of emails or phone calls, the data relating to billions of communications, or—indeed—release a computer virus by way of a bulk equipment interference warrant that affects billions of computers or mobile phones without any requirement that s/he believes that those affected may be involved in criminal activity (including terrorism)."[242]

315. Big Brother Watch argued that "The intelligence agencies have to be able to demonstrate exactly why they need these powers in bulk and what benefit bulk provides rather than the process of requesting data on a specific target in the course of an operation. To date none of this has happened."[243]

316. Witnesses suggested that the Government needed to go further and make an operational case for each of the bulk powers, in the same way that an operational case was published for Internet Connection Records. JUSTICE said that the: "bulk powers in the Draft Bill must be subject to particularly close scrutiny by Parliament and an operational case for each subject to debate and test by the Committee."[244]

317. Apple agreed, saying: "It is extremely difficult to imagine circumstances in which this could be justified, so we believe the bill must spell out in more detail the types of activities required of communications providers and the circumstances in which they are expected to carry them out."[245]

318. Although the majority of witnesses queried the justification for bulk powers, they, like the Committee, were inevitably commenting on the basis of incomplete information. In reflecting on the case for bulk powers, we bore in mind the fact that the ISC have had access to material which is not in the public domain and that they have found it to make a persuasive case for these powers being maintained.[246]

319. ***We recommend that the Government should publish a fuller justification for each of the bulk powers alongside the Bill. We further recommend that the examples of the value of the bulk powers provided should be assessed by an independent body, such as the Intelligence and Security Committee or the Interception of Communications Commissioner. (Recommendation 23)***

320. The bulk interception and bulk equipment interference powers are limited to collecting information about individuals outside the British Islands. Bulk interception is of overseas-related communications, sent by or received from people outside the British Islands, while bulk equipment interference must be for overseas-related communications, information or equipment data.

EMBARGOED until 09.00 on 11 February 2016

242 Written evidence from Article 19 (IPB0052)
243 Written evidence from Big Brother Watch (IPB0007)
244 Written evidence from JUSTICE (IPB0148)
245 Written evidence from Apple Inc. and Apple Distribution International (IPB0093)
246 Intelligence and Security Committee (ISC), *Privacy and Security: A modern and transparent legal framework*, 12 March 2015, HC 1075

321. Liberty questioned how meaningful these definitions would be in practice. They said:

> "the ISC has recently confirmed that Government considers that an "external communication" occurs every time a UK based person accesses a website located overseas, posts on a social media site overseas such as Facebook, uses overseas cloud storage or uses an overseas email provider such as Hotmail or Gmail. Searches on Google are counted as an external communication."[247]

322. Privacy International said similarly that:

> ""Bulk" hacking under Part 6, Chapter 3 is permitted only where the main purpose of the warrant is to obtain "overseas-related" communications, private information and equipment data. This limitation should provide little comfort for those residing in the UK. For instance, much of our data is stored overseas in servers operated by telecommunications services such as Google and Facebook."[248]

323. ***We recognise that, given the global nature of the internet, the limitation of the bulk powers to "overseas-related" communications may make little difference in practice to the data that could be gathered under these powers. We recommend that the Government should explain the value of including this language in the Bill. (Recommendation 24)***

Legality of bulk powers

324. Many witnesses contested the assertion of the Home Office that these powers could be considered legal, not least because of the level of intrusiveness that they could involve.

325. The Bar Council told us:

> "these warrants may be non-specific as to individuals or locations or equipment. The question will be whether applications for such warrants can satisfy the tests of necessity and proportionality. Bulk search warrants or bulk arrest warrants would not. A high level of justification should be required for these bulk warrants to determine why focused warrants with the power to amend and extend in the light of information gathered would not be sufficient in order to satisfy the tests of necessity and proportionality."[249]

326. Privacy International said that:

> "The sheer breadth of a bulk warrant inherently frustrates a substantive review of its necessity and proportionality … bulk warrants need not "specify or target the communications, data or equipment of a particular person, premises or even an organisation." They need only "state the operational purposes for which data need to be obtained, and the IP Bill expressly notes that these can be 'general purposes'" (see Clauses 111(4), 125(4), 140(5)). This lack of specificity—i.e. the absence of any assessment of suspicion—is intrinsically disproportionate and runs afoul of explicit guidance from the ECtHR."[250]

247 Written evidence from Liberty (IPB0143)
248 Written evidence from Privacy International (IPB0120)
249 Written evidence from the Bar Council (IPB0134)
250 Written evidence from Privacy International (IPB0120)

EMBARGOED until 09:30 on 11 February 2016

327. Similar points were made by the Institute for Human Rights and Business who said that:

> "We believe there are still many outstanding questions as to whether collecting and retaining communications in bulk is compatible with the protection of the right to privacy, as outlined in Article 17 of the International Covenant on Civil and Political Rights (ICCPR), Article 8 of the European Convention of Human Rights and Article 8 of the Human Rights Act."[251]

328. Amnesty International UK said that:

> "indiscriminate mass surveillance is never a proportionate interference with the rights to privacy and freedom of expression (articles 8 and 10 ECHR) and can thus never be lawful under the Human Rights Act 1998 and/or ECHR. The interception, analysis or other use of communications in a manner that is neither targeted nor based on a reasonable suspicion that an individual or specific location is sufficiently closely linked to conduct that must legitimately be prevented, is disproportionate."[252]

329. The Home Secretary, in her evidence to the Committee, said firmly that these powers were not about mass surveillance:

> "The UK does not undertake mass surveillance. We have not undertaken, and we do not undertake, mass surveillance. That is not what the Investigatory Powers Bill is about … I would wish to be very clear that mass surveillance is not what we are talking about."[253]

330. The European Court of Human Rights recently considered the use of surveillance powers and the level of specificity needed to ensure interception powers were not used arbitrarily. It concluded that to ensure the tests of necessity and proportionality had been properly applied the interception authorisation must clearly identify:

> "a specific person to be placed under surveillance or a single set of premises as the premises in respect of which the authorisation is ordered. Such identification may be made by names, addresses, telephone numbers or other relevant information."[254]

331. **It is possible that the bulk interception and equipment interference powers contained in the draft Bill could be exercised in a way that does not comply with the requirements of Article 8 as defined by the Strasbourg court. It will be incumbent upon the Secretary of State and judicial commissioners authorising warrants, and the Investigatory Powers Commissioner's oversight of such warrants, to ensure that their usage is compliant with Article 8.**

Effectiveness of bulk powers

332. The Committee heard from representatives of the security and intelligence agencies that they believe these powers are useful and necessary. The Home Secretary gave an

251 Written evidence from the Institute for Human Rights and Business (IPB0094)
252 Written evidence from Amnesty International UK (IPB0074)
253 Q 271 (Theresa May)
254 European Court of Human Rights, *Zakharov v Russia* (2015) application no. 47143/06, para. 264

EMBARGOED until 09:30 on 11 February 2016

explanation of the value of the bulk powers in her written evidence.[255] She said that bulk interception was a "vital tool designed to obtain foreign-focused intelligence and identify individuals, groups and organisations overseas that pose a threat to the UK" which had been used to disrupt terrorist attacks in Europe and identify paedophiles.[256] Bulk equipment interference was described as "facilitating target discovery" in the "increasing number of circumstances where interception is simply not possible or effective", while bulk communications data had proved valuable for MI5 in order to "thwart a number of attacks here in the UK."[257]

333. A few witnesses supported the powers. The BCS said "in the interests of national security a credible argument can be made for the security and intelligence services to undertake both targeted and bulk equipment interference" and they understood "the operational and technical for need accessing communications data in bulk."[258]

334. Other witnesses suggested that the powers were counterproductive because the scale of their potential use meant that it would be impossible to assess the data collected adequately. Ray Corrigan argued that:

> "The whole Investigatory Powers Bill approach to signals intelligence—giant magic computerised terrorist catching machine that watches everyone and identifies the bad guys—is flawed from a mathematical as well as operational perspective… Because of the base rate fallacy and the fact that terrorists are relatively few in number compared to the population as a whole, mass data collection, retention and mining systems, such as those proposed in the IP Bill, always lead to the swamping of investigators with false positives, when dealing with a large population."[259]

335. William Binney, a former Technical Director of the United States National Security Agency, told the Committee that the volume of data gathered by the NSA in America led to analysts being "overloaded", making it impossible for them to focus effectively and identify the real threats.[260] Of bulk collection, he said that:

> "it is not helpful to make the haystack orders of magnitude bigger, because it creates orders of magnitude of difficulty in finding the needle. That is really the issue. Using a targeted approach would give you the needles, and anything closely associated with them, right from the start. That is a rich environment to do an analysis on, and it would help the analysts to succeed in predicting intentions and capabilities."[261]

336. The needle in a haystack analogy was also presented by a number of other witnesses opposed to bulk data collection and analysis.[262] The analogy was challenged by David Wells, a former GCHQ analyst, who said that:

EMBARGOED until 09:30 on 11 February 2016

255 Written evidence from Theresa May MP (IPB0165)
256 *Ibid.*
257 *Ibid.*
258 Written evidence from BCS, The Chartered Institute for IT (IPB0075)
259 Written evidence from Mr Ray Corrigan (IPB0053)
260 Written evidence from William Binney (IPB0009)
261 Q 239 (William Binney)
262 For example, written evidence from Eris Industries Limited (IPB0011), Giuseppe Sollazzo (IPB0032), Krishan Bhasin (IPB0034), Mr Eric King (IPB0106), Privacy International (IPB0120) and Dr Julian Huppert (IPB0130)

> "I would first recommend that the Committee re-consider the needle/haystack analogy typically used when discussing intelligence agency use of bulk datasets. Instead, consider how you and millions of others use the Google search engine, and how much Google—like the ability of intelligence agencies to process big data—has changed over the past 15 years.
>
> Initially, Google only allowed relatively simple search terms. Many businesses had little or no internet presence, while Google's 'web-crawling' technology did not necessarily access all those that did. In short, it lacked a comprehensive dataset to query, and as a result, it was difficult to use with confidence. These data inconsistencies meant that you could not be certain that Google had access to the data you were looking for, or whether the results it pulled back were relevant to your initial query. Like the intelligence analyst described by Mr Binney, you were confronted by too much irrelevant data. Even after clicking through multiple pages of results, you might not find what you were looking for; an alternative, more targeted method (say a local phone book) was often more effective." [263]

337. Mr Wells went on to explain that, given the growth of the internet and its role in everyday life, the bulk data collected by Google has made it increasingly accurate and facilitates "the ability to ask complex and nuanced questions" which reduces the number of results returned and increases their relevance. He said that the same was true for intelligence analysts and their use of bulk data and that therefore they are not overwhelmed.[264]

338. Paul Bernal argued that the automated processing required to facilitate such big data analysis comes with additional risks:

> "Further vulnerabilities arise at the automated analysis stage: decisions are made by the algorithms, particular in regard to filtering based on automated profiling. In the business context, services are tailored to individuals automatically based on this kind of filtering—Google, for example, has been providing automatically and personally tailored search results to all individuals since 2009, without the involvement of humans at any stage. Whether security and intelligence services or law enforcement use this kind of a method is not clear, but it would be rational for them to do so: this does mean, however, that more risks are involved and that more controls and oversight are needed at this level as well as at the point that human examination takes place."[265]

339. David Wells concluded that bulk and targeted powers, far from being mutually exclusive, were complementary and "mutually beneficial".[266]

340. **We are aware that the bulk powers are not a substitute for targeted intelligence, but believe that they are an additional resource. Furthermore, we believe that the security and intelligence agencies would not seek these powers if they did not believe they would be effective and that the fact that they have been operating for some time would give them the confidence to assess their merits.**

263 Written evidence from David Wells (IPB0166)
264 *Ibid.*
265 Written evidence from Dr Paul Bernal (IPB0018)
266 Written evidence from David Wells (IPB0166)

EMBARGOED until 09:30 on 11 February 2016

341. **National security considerations mean that we are not well-placed to make a thorough assessment of the value of the bulk powers. The scrutiny and conclusions of the Intelligence and Security Committee on the Bill will be of significant assistance for Parliamentarians considering these powers.**

342. We make a further recommendation on the automated analysis of bulk datasets in para 703.

Safeguards for bulk powers

343. Witnesses also suggested that there were insufficient safeguards for the bulk powers proposed. Article 19 said that:

> "Nothing in Part 6 or, indeed, elsewhere in the draft Bill imposes any kind of upper limit on what might be obtained by way of a bulk warrant, subject only to the requirement that the Secretary of State considers that it is "necessary" in the interests of national security or certain other specified interests (Clauses 107(1)(b)), 122(1)(a), and 137(1)(b))."[267]

344. The Equality and Human Rights Commission called for more attention to "be given to safeguards that clearly limit the basis on which bulk material can be examined and that will ensure safe retention and destruction of material. Such safeguards might include more narrowly defined purposes."[268]

345. Dr Tom Hickman has suggested that: "At a minimum in my view the Joint Committee should insist on:

> (1) Tighter protections for persons in the UK particularly in relation to use of communications data requiring at least operationally independent authorization for use of such data together with JC approval where this would be required for police obtaining communications data.
>
> (2) Requiring warrants to be more narrowly focused as to their purpose and permitted search criteria. The Act could require that the purposes will be specified as tightly as is operationally reasonable.
>
> (3) Bringing safeguards currently in the Code to legislation and other matters on record-keeping and destruction from internal policy to legislation."[269]

346. In the Guide to Powers and Safeguards accompanying the draft Bill, the Home Office said that the following safeguards exist for bulk powers:

- The ability to seek bulk warrants will be limited to the security and intelligence agencies.
- The issue of a bulk warrant must be necessary in the interests of national security.
- Bulk interception and equipment interference warrants must be focused on obtaining data relating to persons outside the UK.

267 Written evidence from Article 19 (IPB0052)
268 Written evidence from the Equality and Human Rights Commission (IPB0136)
269 Written evidence from Dr Tom Hickman (IPB0039)

EMBARGOED until 09:30 on 11 February 2016

- Bulk warrants will only come into force once they have been authorised by the Secretary of State and approved by a Judicial Commissioner.
- Access to any data obtained under a bulk warrant must be necessary for a specific operational purpose approved by the Secretary of State and a Judicial Commissioner.
- Additional safeguards will apply in respect of content acquired under bulk interception and bulk equipment interference warrants relating to persons in the UK.
- Additional safeguards are provided for the acquisition and use of bulk personal datasets by the security and intelligence agencies.[270]

347. In a letter to the Committee, the Home Secretary provided additional information on the safeguards for bulk powers in the draft Bill.[271] **We are grateful to the Home Secretary for the additional information she provided on safeguards for bulk powers, but note that her letter arrived too late for other witnesses to give the Committee their views upon it.**

348. **In general, we are content that the safeguards proposed by the Home Office, buttressed by authorisation by Judicial Commissioners and oversight from the Investigatory Powers Commissioner will be sufficient to ensure that the bulk powers are used proportionately.**

349. **We acknowledge, though, the call for greater safeguards for the bulk powers. We believe that it is difficult to make a thorough assessment of the effectiveness of further safeguards without a greater understanding of the way in which bulk powers are operated in practice.** ***We recommend that the Investigatory Powers Commissioner, within two years of appointment, should produce a report to Parliament considering the safeguards that exist and making recommendations for improvements if required. (Recommendation 25)***

Bulk interception

350. Clause 106 (2) provides for the obtaining of "related communications data" from within "overseas-related communications" captured by bulk interception activities. Related communications data is defined as data related to the intercepted communication, its sender or recipient, or the telecommunications service used that can be separated from the content of the communication.

351. A similar provision on related communications data obtained from targeted interception exists in Clause 12.

352. Witnesses who commented on related communications data argued that the term was not sufficiently clear. Privacy International said:

> "If content is defined based on the conveyance of meaning, it is unknown to us how 'related communications data' could be part of content in the first place. The Home Office needs to be clearer on how these definitions interact with the technical specifications of communications. For instance, intercepting

270 Home Office, *Draft Investigatory Powers Bill: Guide to Powers and Safeguards*, Cm 9152, November 2015, p.22
271 Written evidence from Theresa May MP (IPB0165)

EMBARGOED until 09:30 on 11 February 2016

at an ISP on port 25 will give access to a communication (e.g. an email) but the "content" (email body) will include the communications data of the email (email headers)."[272]

353. Graham Smith suggested that:

"The Home Office could usefully produce a comprehensive list of datatype examples, where appropriate with explanations of context, categorised as to whether the Home Office believes that each would be entity data, events data, contents of a communication, data capable of being related communications data when extracted from the contents of a communication and so on."[273]

354. The written evidence from the Home Office explained that:

"Related communications data and equipment data are non-content data obtained under interception warrants and equipment interference warrants respectively. These data are wider than the categories of data that can be obtained by means of a communications data authorisation (i.e. they include but are not limited to communications data).

Distinguishing these data from content means that appropriate safeguards and handling safeguards can be consistently applied: for example, the Secretary of State may specify that a bulk interception warrant should authorise the obtaining of related communications data only, and that any content acquired under that warrant should not be made available for subsequent examination.

Both related communications data and equipment data can include communications data and any systems data which enables or otherwise facilitates the functioning of any system or service provided by the system. Systems data is not content. It is also possible for certain structured data types to be extracted from the content of a communication or an item of private information under a warrant. All related communications data and equipment data so obtained will be subject to the handling safeguards set out in the draft Bill.

These definitions are a balance between meeting the operational requirements of the intelligence agencies to protect the public from terrorists and serious criminals, while protecting the most private information with stringent safeguards. The definitions are also sufficiently robust and technology neutral to cater for new technologies that come online as the internet adapts and changes."[274]

355. The Open Rights Group expressed concern about extracting of communications data from intercepted communications, on the basis that such data is more amenable for automated analysis. They said:

"We would also urge caution about the powers … to extract data from content, presumably email addresses or calendar events. Treating such content as data

272 Written evidence from Privacy International (IPB0120)
273 Written evidence from Graham Smith (IPB0126)
274 Written evidence from the Home Office (IPB0146)

EMBARGOED until 09:30 on 11 February 2016

> would enable the automated analysis of such materials, and the implications should be explained in more detail."[275]

356. The report of the Intelligence and Security Committee suggested that such analysis of related communications data was the primary value in undertaking bulk interception:

> "We were surprised to discover that the primary value to GCHQ of bulk interception was not in reading the actual content of communications, but in the information associated with those communications. This included both Communications Data (CD) as described in RIPA … and other information derived from the content (which we refer to as Content-Derived Information, or CDI), including the characteristics of the communication … While CDI is not what might be most obviously understood to be content, under RIPA it must be treated as content, not CD. Examination of CDI therefore requires the same Ministerial authority as examination of content."[276]

Bulk acquisition of communications data

357. Part 6 Chapter 2 of the draft Bill provides for the security and intelligence agencies to acquire bulk communications data about people in the British Islands for the purposes of preventing or detecting serious crime and the bulk CD of people overseas where it is in the interests of the economic well-being of the UK in so far as it is relevant to national security.

358. Although we note that international practices vary, and that in the USA there have been moves away from bulk acquisition of communications data by US intelligence services, the Intelligence and Security Committee made the case for UK agencies to have this capability.[277]

359. There were particular concerns among witnesses about the intrusiveness of bulk communications data. One of the most common arguments for this was that communications data is more suitable to be aggregated and analysed in bulk, whereas content is harder for computers to reliably process in this way. Dr Tom Hickman said:

> "It is now becoming widely accepted that, when aggregated, communications data are more revealing and intrusive then content data—identifying a person's contacts and associations, websites visited (up to the first slash), providing information about habits and preferences and even tracking a person's movements."[278]

360. Dr Glyn Moody explained that:

> "The distinction between "content" and "communications data" is meaningless, and again betrays an ignorance of how modern digital systems work. "Communications data" is metadata; the only difference between metadata and data is that metadata is pre-sorted into conceptual categories—

275 Written evidence from Open Rights Group (IPB0108)

276 Intelligence and Security Committee (ISC), *Privacy and Security: A modern and transparent legal framework*, 12 March 2015, HC 1075, para 80

277 Intelligence and Security Committee (ISC), *Privacy and Security: A modern and transparent legal framework*, 12 March 2015, HC 1075

278 Written evidence from Dr Tom Hickman (IPB0039)

EMBARGOED until 09:30 on 11 February 2016

> sender, date, location, email address etc.—while content is unsorted. As such, metadata is hugely more valuable than content, because it can instantly be combined with other metadata; indeed, the power of computers today is such that it can be combined with billions of other metadata elements. Content, by contrast, is largely useless for this purpose, because computers cannot understand it. Before it can be used, it must be parsed—texts must be "read", images "seen." Currently, those are very hard computing tasks; that means content is not useful for scalable analysis (although it is valuable for human-based scrutiny, but does not scale.) So the idea that "communications data" is somehow less intrusive than gathering content is not just wrong, but exactly wrong: it is hugely more intrusive, which is why it should never be gathered routinely, as proposed here."[279]

361. The Global Network Initiative concluded that:

> "bulk collection of communications data—both content and metadata—threatens privacy and freedom of expression rights and undermines trust in the security of electronic communications services provided by companies. This practice is incompatible with the principles of necessity and proportionality that the legal frameworks for communications surveillance must meet to ensure they are consistent with human rights standards."[280]

362. **We agree that bulk communications data has the potential to be very intrusive. As with the other bulk powers, we believe that the fuller justification which we have recommended the Government produces (see para 319) and the conclusions of the Intelligence and Security Committee on the Bill will assist Parliament's consideration of the necessity and appropriateness of bulk acquisition.**

Bulk equipment interference

363. The Committee heard concerns about the security risks of undertaking equipment interference, both targeted and bulk. Big Brother Watch said that:

> "Given the clear risks involved, the proportionality of the tactic needs to be considered. Equipment interference should not be used as a bulk tactic designed to infiltrate broader systems, networks or organisations."[281]

364. Wendy Grossman told the Committee that:

> "It is not possible to create vulnerability—a hole—in such equipment that only "good guys" or "our side" can use. Adding vulnerabilities to widely used equipment will make Britain's infrastructure vulnerable and aid those who wish to attack Britain by providing additional paths they can use to do it."[282]

365. CSPs expressed concern that they would have to weaken their systems in order to comply with EI warrants. The joint evidence submitted by Facebook, Google, Microsoft, Twitter and Yahoo said:

279 Written evidence from Dr Glyn Moody (IPB0057)
280 Written evidence from Global Network Initiative (IPB0080)
281 Written evidence from Big Brother Watch (IPB0007)
282 Written evidence from Wendy M. Grossman (IPB0068)

EMBARGOED until 09:30 on 11 February 2016

> "There are no statutory provisions [in the draft Bill] relating to the importance of network integrity and cyber security, nor a requirement for agencies to inform companies of vulnerabilities that may be exploited by other actors. We urge the Government to make clear that actions taken under authorization do not introduce new risks or vulnerabilities for users or businesses, and that the goal of eliminating vulnerabilities is one shared by the UK Government. Without this, it would be impossible to see how these provisions could meet the proportionality test."[283]

366. Vodafone similarly pointed out that:

> "Operators within the UK (and Europe) have obligations to ensure the security of their networks and services, and the resiliency of their networks and, more importantly, a commercial imperative to do so: it is fundamental that our services are secure and reliable to compete in the market. As such, an obligation to assist with EI must not require an operator to lessen the standard of its general security, or which could adversely impact the resiliency of its network."[284]

367. CSPs and others were concerned not just at the threat to their systems but the possibility of their employees being required to participate in EI activities. Apple said that "the bill as it stands seems to threaten to extend responsibility for hacking from Government to the private sector".[285] Virgin Media said:

> "The role of CSPs in EI is not made clear in the draft Bill. We believe there needs to be full consultation with CSPs in advance of any EI warrant or technical capability notice being imposed, for example to guard against EI having a negative impact on networks or customers. As drafted, no consultation appears to be required before the imposition of EI warrants. The draft Bill also creates the possibility CSP's employees may be required to actively assist in EI operations, perhaps to seek out vulnerabilities for exploitation or develop vulnerabilities, which we do not believe is appropriate."[286]

368. Mozilla told us that, in terms of open source software, such a requirement would not work, as the open source community would identify any attempt to compromise a program.[287]

369. Professor John Naughton and Professor David Vincent warned of the risks of unintended consequences, particularly as technology develops:

> "the most worrying concern is that as the 'Internet of Things' expands, and billions of devices become networked, bulk EI could have unintended consequences which might prove very counter-productive to the interests of the UK."[288]

EMBARGOED until 09:30 on 11 February 2016

283 Written evidence from Facebook Inc., Google Inc., Microsoft Corp., Twitter Inc. and Yahoo Inc. (IPB0116)
284 Written evidence from Vodafone Ltd (IPB0127)
285 Written evidence from Apple Inc. and Apple Distribution International (IPB0093)
286 Written evidence from Virgin Media (IPB0160)
287 Written evidence from Mozilla (IPB0099)
288 Written evidence from Professor John Naughton and Professor David Vincent (IPB0131)

370. Witnesses suggested that involving the private sector in EI activities would have negative consequences. Professor Ross Anderson said:

> "if the powers are abused, or seen as capable of being abused, there could be exceptionally serious damage to British industry. If people overseas come to the conclusion that, if they buy a security product from a British firm, it may have a GCHQ mandated back door, they will not buy it; they will buy from a German firm instead."[289]

371. Similar arguments were put forward in relation to encryption (see para 260).

372. ***We recommend that applications for targeted and bulk EI warrants should include a detailed risk analysis of the possibilities of system damage and collateral intrusion and how such risks will be minimised. We also recommend that such warrants should detail how any damaged equipment will be returned to its previous state at the point that the authorisation or operational need ceases. (Recommendation 26)***

373. **We acknowledge the concerns of CSPs and other companies who may be required to be complicit in EI activities. We believe that, on balance, it is necessary, subject to a warrant that has been authorised as necessary and proportionate by the Secretary of State and a Judicial Commissioner.**

374. ***We recommend that the Code of Practice on equipment interference should set out how individuals and companies should be engaged with when conducting authorised EI activities to make the process more transparent and foreseeable. (Recommendation 27)***

Bulk personal datasets

Overview

375. Clauses 150 to166 provide for the security and intelligence agencies to acquire and examine Bulk Personal Datasets (BPDs).

376. BPDs are sets of personal information about a large number of individuals, alive and dead, the majority of whom will not be of any interest to the security and intelligence agencies. The datasets are held on electronic systems for the purposes of analysis by the security and intelligence agencies. The examples provided by the Home Office were the telephone directory, the electoral roll, and data about individuals assessed to have access to firearms.[290]

377. The Security and Intelligence agencies currently have powers under the Security Service Act 1989 and the Intelligence Services Ac 1994 to acquire and use BPDs to help them fulfil their statutory functions, including protecting national security. BPDs may be acquired using investigatory powers, from other public sector bodies or commercially from the private sector.

378. This was not a view shared by Matthew Ryder QC. "Part 7, on bulk data sets, is essentially new, has not been regulated before and is not in the existing legislation in

289 Q 79 (Professor Ross Anderson)
290 Written evidence from the Home Office (IPB0159)

EMBARGOED until 09:30 on 11 February 2016

any meaningful way. The power to have access to bulk data sets and how they would be defined is something new."[291]

379. The Home Office has said that the use of BPDs is already subject to stringent internal handling arrangements and that the regime is overseen by the Intelligence Services Commissioner.[292] The Home Office also said that the Bill will significantly enhance the safeguards that apply to the acquisition and use of BPDs.[293]

Support for BPDs

380. In her evidence to the Committee, the Home Secretary said that BPDs were "a critical part of [the agencies'] response to the increasingly complicated and challenging task of defending the UK's interests and protecting its citizens in a digital age."[294] She identified the value of BPDs in facilitating protection at major events, such as the NATO Summit in Wales in 2014 and London Olympics in 2012, preventing terrorist access to firearms and identifying foreign fighters.[295]

381. There was some support among witnesses for the use of BPDs.[296] The BCS said that they recognise "the need for the use of bulk personal datasets by the security and intelligence services in undertaking their legitimate surveillance role on behalf of national security",[297] while Amberhawk Training Ltd said that the retention and use of BPDs was workable provided that the full protection of the Data Protection Act be afforded to the personal data of innocent people.[298]

382. The agencies' use of bulk personal datasets is subject to regular audit and inspection by the Intelligence Services Commissioner. The current Commissioner, Sir Mark Waller, told the Committee that "the present system works very well and provides safeguards."[299]

Opposition to BPDs

383. A number of witnesses argued that the Government had not made the case sufficiently to support BPDs.[300] Liberty said that:

> "No argument is even attempted that BPDs are necessary or proportionate for Article 8 HRA purposes. The ISC reported that the Agencies told them that BPDs are an 'increasingly important investigative tool' to 'enrich' information obtained through other techniques and concludes that BPDs are 'relevant' to national security investigations. "Enriching" and "relevant" does not meet the legal threshold for lawfulness."[301]

384. Eric King said that:

291 Q 186 (Matthew Ryder QC)
292 Home Office, *Draft Investigatory Powers Bill: Guide to Powers and Safeguards*, Cm 9152, November 2015, para 71
293 *Ibid.*, para 72
294 Written evidence from Theresa May MP (IPB0165)
295 *Ibid.*
296 See, for example, written evidence from Professor Anthony Glees (IPB0150)
297 Written evidence from BCS, The Chartered Institute for IT (IPB0075)
298 Written evidence from Amberhawk Training Ltd (IPB0015)
299 Q 39 (Sir Mark Waller)
300 For example, written evidence from Privacy International (IPB0120)
301 Written evidence from Liberty (IPB0143)

EMBARGOED until 09:30 on 11 February 2016

> "the Government, in my mind, should make operational cases from first principles for every single one of these powers. Simply because they have already been in use and simply because the agencies have interpreted law in a manner that they feel has made them lawful does not make them lawful. It is right that Parliament should receive a full operational case for each and every one of these powers. It is a matter of assessing not whether they are merely helpful or offer some form of value, but whether, given the scope of everyone's lives that they touch—after all, that is what bulk powers do—they can be vetted and scrutinised to make sure that they are both necessary and proportionate."[302]

385. The Institute for Human Rights and Business agreed that "An objective assessment of the necessity and proportionality" was required. The Institute suggested that "the broad use of bulk powers and class based warrants which are likely to collect personal information of individuals not suspected of any crime and in such volume makes the necessary and proportionate test extremely difficult, if not impossible to conduct."[303] A similar argument was made by the Open Rights Group.[304]

386. In a letter to the Committee, the Home Secretary set out further the case for the bulk powers including BPDs with examples of how they have proved valuable in practice.[305] This information arrived too late in the process for other witnesses to comment upon it.

387. Concerns were also raised about the risks of acquiring and examining BPDs. The Information Commissioner's Office said that "Given the increasing amounts of personal data generated and held in data sets this could be a particularly far reaching and intrusive provision."[306]

388. The evidence submitted by Mr. Bernard Keenan, Dr. Orla Lynskey and Professor Andrew Murray suggested that:

> "The decisions and risk factors produced by analysis of Bulk Personal Datasets threaten personal autonomy and risk producing systemic discrimination, stereotyping, and biased decisions, both at the policy level and operational level. Individuals at home in the UK or abroad will have no control over the type of processing of their personal information that the agencies carry out for authorized purposes."[307]

389. **We are grateful to the Home Secretary for the additional information provided to the Committee. We believe that that the lack of a formal case for bulk personal datasets (BPDs) remains a shortcoming when considering the appropriateness of this power.**

390. ***We recommend that the Home Office should produce its case for bulk personal datasets (BPDs) when the Bill is published. (Recommendation 28)***

391. ***We recommend that the Intelligence and Security Committee, in their analysis of BPDs, should assess the extent to which the concerns expressed by witnesses are justified. (Recommendation 29)***

302 Q 207 (Eric King)
303 Written evidence from the Institute for Human Rights and Business (IPB0094)
304 Written evidence from Open Rights Group (IPB0108)
305 Written evidence from Theresa May MP (IPB0165)
306 Written evidence from the Information Commissioner's Office (IPB0073)
307 Written evidence from Mr. Bernard Keenan, Dr. Orla Lynskey and Professor Andrew Murray (IPB0071)

EMBARGOED until 09:30 on 11 February 2016

Lack of information about BPDs

392. Many witnesses who commented on BPDs argued that it was not apparent from the draft Bill what information the datasets might include. Dr Tom Hickman said that it was "far from clear from the Bill's documents how far this extends—medical records? Immigration histories? Tax returns? Court records?—and what about privately generated data sets such as company employee records or bank account details?"[308]

393. medConfidential agreed that "There is no clarity on the use of bulk personal datasets by the security and the intelligence agencies. There is only a description that they may be collected, and kept for as long as the agencies believe they may be useful, and that they be used as warranted."[309]

394. The Information Commissioner's Office complained that the examples provided in the supporting material for the draft Bill were unhelpful because they were already available to the security and intelligence agencies:

> "The examples given in the Guide to Powers and Safeguards refer to telephone directories and the electoral roll. These datasets are already available to various agencies often under specific statutory provisions. For example, Schedule 1 of the Counter-Terrorism Act 2008 amends the Representation of the People (England and Wales) Regulations 2001 to require the supply of the full electoral register to the security services."[310]

395. The Information Commissioner Christopher Graham, expressed his misgivings when giving oral evidence:

> "In the Explanatory Memorandum—the guide to powers and safeguards—the authors of the Bill have chosen some very inapt examples of the sorts of bulk data sets they want to access for reasons of law and order, by giving the telephone directory and the electoral register as the two examples. This is bizarre, because that information is already available. Explicitly, legislation was amended to make sure that that information is available to the security services. It does not require this Bill to provide that. That begs the question of what are these data sets that are so necessary, and we are not told, which then begs the question that if the authorities are not going to tell us what data sets they are going to be accessing, are they prepared to say what data sets they would not be prepared to access?"[311]

396. Witnesses offered competing suggestions as to what BPDs the security and intelligence agencies might or might not have. For example, Professor Ross Anderson said:

> "For starters, we know that the police have access to things like credit reference and DVLA records. That is public knowledge. Secondly, they have access to medical stuff … Thirdly, in any case, hospital medical records were sold on a wide scale in the care.data scandal last year, and it would have been rather negligent if GCHQ had not grabbed a copy on its way past. Fourthly, it is well

308 Written evidence from Dr Tom Hickman (IPB0039)
309 Written evidence from medConfidential (IPB0005)
310 Written evidence from the Information Commissioner's Office (IPB0073)
311 Q 231 (Christopher Graham, Information Commissioner)

EMBARGOED until 09:30 on 11 February 2016

> known that some kinds of bank records, in particular all international financial transactions, are harvested on their way through the SWIFT system."[312]

397. Speaking on the same panel, Professor Sir David Omand took issue with this point:

> "it is important not to allow fantasy to intrude at this point. The central bank governors responsible for the SWIFT system agreed that that system could be searched for specific transactions of known criminals and terrorists. That is public knowledge. All SWIFT data is not scooped up."[313]

398. David Davis MP told the Committee that:

> "they have all the communications data. They have flight data. They almost certainly gave financial data. They may well have ANPR data. This is very intrusive information for a state to hold … Yes, you are right that warranting is good, but frankly the extent to which much of this database should exist is very debateable."[314]

399. Baroness Jones of Moulsecoomb suggested that "There are also, of course, medical records and financial asset records, and so on, in those data sets. It is a very wide scope."[315]

Excluded datasets

400. A number of witnesses proposed that certain types of dataset should be explicitly excluded from collection. The most common suggestion was that medical records should not be part of BPDs, a point made by medConfidential, Amberhawk Training Ltd, Open Intelligence and Mark Dziecielewski.[316]

401. The Information Commissioner explained that:

> "There is very great public concern about various initiatives in the health sector around the care.data project. Patients were very concerned that their most personal and most sensitive information was going to be uploaded into a health service information centre and then shared around rather freely with the insurance companies and heaven knows what. People were very concerned about that. That scheme has now been rethought and that is very good news. But are we being invited to give a blank cheque to the authorities to access everyone's most sensitive health data? I suspect not, but it does not say that in either the legislation or the guide to powers and safeguards."[317]

402. The Committee sought further clarity from the Home Office as to the types of information BPDs might or might not include. In a letter to the Committee, the Rt Hon John Hayes MP, Minister of State for Security, wrote:

EMBARGOED until 09.30 on 11 February 2016

312 Q 92 (Professor Ross Anderson)
313 Q 92 (Professor Sir David Omand)
314 Q 177 (David Davis MP)
315 Q 177 (Baroness Jones of Moulsecoomb)
316 Written evidence from medConfidential (IPB0005), Amberhawk Training Ltd (IPB0015), Open Intelligence (IPB0066) and Mark Dziecielewski (IPB0082)
317 Q 231 (Christopher Graham, Information Commissioner) See, also, written evidence from the Information Commissioner's Office (IPB0073)

> "there is a need to ensure any publication of guidance, or the types of data that the agencies hold, does not jeopardise national security … Further detail as to what is held, or how they are used, could incite behaviour change and reduce the utility of the information itself." He further explained that it is also not possible "to make public the types of datasets that currently the agencies do not hold; this may provide those that wish to do us harm greater insight as to the limits of the agencies' capabilities and thus how to avoid detection or disruption."[318]

403. **While the Committee acknowledges the case made by the Home Office for not providing detailed information as to the contents of bulk personal datasets (BPDs), the lack of that detail makes it hard for Parliament to give the power sufficient scrutiny.**

Safeguards required for BPDs

404. Some witnesses suggested areas where the proposals on BPDs could be improved. Amberhawk Training pointed out that the Government was not taking the opportunity to repeal existing powers to acquire BPDs:

> "All existing powers (i.e. other [than] in the Bill) that could be used by the national security agencies to obtain a bulk personal dataset or communications personal data should be negated. For example, Schedule 1 of Counter-Terrorism Act 2008 which modifies the "Representation of the People (England and Wales) Regulations 2001 (S.I. 2001/341)" is not repealed. This modification includes Regulation 108A which is entitles the "Supply of full register etc to the security services". Not to close down existing powers would mean that there may be a secondary access route that could allow access to personal data outwith the protections in this Bill."[319]

405. Various witnesses suggested that further safeguards were needed for BPDs.[320] Amberhawk Training pointed out that "in Schedule 6 which concerns all Codes of Practice, there is no detail as to what should appear in the BPD Code of Practice. The Committee may wish to press for detail as to the content of the BPD Code as the safeguards appear to be no more than a blank canvass to be completed by the Secretary of State once a future Bill becomes law."[321]

406. **The safeguards for BPDs are not sufficiently explained in the Bill. We have not seen a draft Code of Practice on BPDs, and we therefore do not know whether BPDs will, in practice, be treated differently from the communications datasets that are referred to in parts 4 and 6 of the Bill (and which also appear to fall under the definition of a BPD).**

407. ***We believe that a draft Code of Practice on BPDs should be published when the Bill is introduced to provide greater clarity on the handling of BPDs, not least in relation to the provisions of the Data Protection Act 1998. To the greatest extent possible, the***

EMBARGOED until 09:30 on 11 February 2016

318 Written evidence from the Home Office (IPB0159)
319 Written evidence from Amberhawk Training Ltd (IPB0015)
320 See, for example, written evidence from Simon Pooley (IPB0060), Privacy International (IPB0120) and Dr Julian Huppert (IPB0130)
321 Written evidence from Amberhawk Training Ltd (IPB0015)

safeguards that appear in the Data Protection Act 1988 should also apply to personal data held by the security and intelligence agencies. (Recommendation 30)

408. ***We also agree that existing powers for acquiring BPDs should be consolidated in this Bill and that any other powers for the security and intelligence agencies to acquire BPDs should be repealed. (Recommendation 31)***

EMBARGOED until 09:30 on 11 February 2016

4 Authorisation regimes

Overview

409. This Chapter examines first some of the principles underpinning the more stringent authorisation processes set out in the draft Bill and then addresses the authorisation regimes for each of the capabilities. It also covers issues of extraterritoriality and addresses the provisions regarding privileged communications relating to lawyers, journalists and parliamentarians contained within the draft Bill.

Overarching issues

410. The draft Bill sets out the process of authorisation for each of the capabilities which it legislates for. The process of authorisation for communications data remains largely unchanged and will be dealt with in the specific section below. The draft Bill introduces a new system of authorisation for targeted interception, targeted equipment interference, and all types of bulk warrants. While there are specific issues that relate to the authorisation process for each type of warrant, which will be dealt with below, this section will deal with issues common to the authorisation of all of these warrants which are subject to the more stringent authorisation procedure.

Judicial Authorisation

411. The draft Bill introduces an extra layer of judicial authorisation for powers that have previously been subject to ministerial authorisation only. This procedure, described by the Government as a "double lock"[322] applies to warrants for targeted interception, targeted equipment interference, and all forms of bulk warrants.

412. Initial political reaction to this announcement was positive, with the Shadow Home Secretary acknowledging that the draft Bill "has brought forward much stronger safeguards, particularly in the crucial area of judicial authorisation."[323]

413. Many witnesses were also positive about the decision to introduce a judicial element to the authorisation process. Peter Gill, for example, said:

> "Clearly the draft bill is an improvement on the current authorisation situation because it involves judges in the approval of warrant applications and thus adds a judicial dimension to the 'political' decision made by ministers. This is appropriate because the determination as to whether an application passes the triple test of legality, necessity and proportionality as required by the Human Rights Act is, finally, a legal question."[324]

414. Submissions to the Committee fell into three camps on this issue: those who thought authorisation should be undertaken by Ministers only; those who thought authorisation should be undertaken by judges only; and those who were content with a mixed approach (as taken by the draft Bill), although some witnesses in this group were concerned by the judicial review restriction (which we address below).

322 HC Deb, 4 November 2015, col 969
323 HC Deb, 4 November 2015, col 973
324 Written evidence from Peter Gill (IPB0008)

EMBARGOED until 09.30 on 11 February 2016

415. Both Lord Carlile of Berriew CBE QC and the Rt Hon Owen Paterson MP made the case for authorisation decisions to remain with ministers only. Lord Carlile argued that ministers are accountable for their actions in a way that judges cannot be:

> "Ministers are accountable to Parliament. This includes accountability to Select Committees, to the relevant House, and ultimately to their electorate. Ministers seen to be inefficient or troublesome can be reshuffled at short or even no notice. It is not the normal or even acceptable role of a judge to make executive decisions. They are not elected, and rarely removed."[325]

416. Similarly, Mr Paterson referred to the separation of powers in his evidence to the Committee:

> "Go back to Montesquieu and the separation of powers. Their skill is interpreting law or, here, interpreting the manner in which a law has been put into action by an Executive. I feel very strongly that these are executive decisions. They are operational decisions and must be made by a democratically elected Minister, accountable to Members of Parliament."[326]

417. The Rt Hon Lord Blunkett believed "that we need to find a way of ensuring that a tandem process can work, simply because there is an atmosphere now, driven by those who suspect the state of all sorts of things, that makes it very difficult to resile from what has been put forward."[327]

418. The Committee also received submissions which argued instead that all or some categories of warrants should be authorised by judges without any element of ministerial decision-making.[328] Big Brother Watch questioned the relevance of the accountability argument on the basis that "no Secretary of State has ever explained their actions in relation to a warrant before Parliament, posing the question of strength of democratic accountability".[329]

419. We are aware that particular sensitivities around these issues may apply in Northern Ireland. The Government will need to reflect on these sensitivities as this legislation progresses.

EMBARGOED until 09:30 on 11 February 2016

325 Written evidence from Lord Carlile of Berriew CBE QC (IPB0017)
326 Q 96 (Owen Paterson MP)
327 Q 97 (Lord Blunkett)
328 See, for example, written evidence from Big Brother Watch (IPB0007), Mr Ray McClure (IPB0016), Article 19 (IPB0052), Bingham Centre for the Rule of Law (IPB0055), Dr Glyn Moody (IPB0057), Amnesty International UK (IPB0074), Paul Biggs (IPB0084), Privacy International (IPB0120), Law Society of Scotland (IPB0128), Liberty (IPB0143) and JUSTICE (IPB0148)
329 Written evidence from Big Brother Watch (IPB0007)

Box 3: International comparisons

The capacity of police and security services to access communications and, in particular, the degree of judicial authorisation involved varies significantly between nations and, within nations, between different types of information.

The Committee was grateful to receive evidence from Sir Bruce Robertson, New Zealand Commissioner of Security Warrants, whose role closely resembles that of the Judicial Commissioner proposed in the draft Bill in terms of authorisation. He explained that, with respect to the interception of communications, "when there is a desire on the part of either the security service or the [The Government Communications Security Bureau (GCSB)] to get authorisation, they make an application to the relevant Minister but the Act provides that the relevant Minister can grant an authorisation only if I concur with the granting of it. It is an entirely dual operation. From my experience of three years and the experience of my predecessor, who was in office for almost 14 years, this appears to provide a sensible and operational joint protective measure."[330]

At one end of the spectrum are Australia and France. In Australia, no judicial authorisation is required for the police and security services to access information. Only where access is sought to a journalist's metadata is a warrant required. Nor is any judicial oversight or authorisation required in France. The Prime Minister can authorise data interception on the basis of some very broad grounds such as the protection of major foreign policy, economic, and scientific interests or the prevention from 'organised delinquency'. Before authorisation can be given, the National Committee of Intelligence Techniques Control must be consulted, but its decisions are only advisory and not binding on the Prime Minister.

In other countries some form of judicial authorisation is more common. To intercept communications, the Canadian police must apply to a superior court for a warrant, which would also need to be counter-signed by the relevant provincial Attorney-General. Applications for warrants must specify the reason for the application. There is a different authorisation procedure for the Canadian security services who must apply to a member of a panel of Federal Court judges with security clearance.

The situation relating to metadata in Canada is rather less clear. It is the subject of ongoing political controversy and is evolving rapidly. The Criminal Code prohibits the interception of private communications without a warrant, but as the security services have not regarded metadata as "private" they have seemingly collected and used it with limited constraint: in evidence to the Standing Senate Committee on National Security and Defence, the Prime Minister's National Security Advisor stated that metadata "does not represent a compromise of private communications by Canadians. It is data about data, so it is well within the legal parameters of [Communications Security Establishment Canada's (CSEC)] operations".

In New Zealand, as in Canada, the law relating to the collection and retention of metadata has been rather less developed, and not subject to the same sorts of controls. In both Canada and New Zealand, the warrant system only relates to domestic interception and security agencies are free to conduct overseas surveillance without further authorisation.

330 Q 250 (Sir Bruce Robertson)

EMBARGOED until 09:30 on 11 February 2016

In Canada in particular, there have been concerns about the extent to which Canadians have been 'inadvertently' included in overseas data gathering.

In the USA, the Freedom Act 2015 provided some restrictions on the powers of surveillance that the National Security Agency had had under the Patriot Act 2015. CSPs are now required to store telephony metadata which the NSA can apply for a warrant to access where they were previously required to hand the information directly to the NSA.

Source: House of Commons Scrutiny Unit

420. David Anderson QC pointed out that, at least in relation to police warrants, it is questionable whether there needs to be a ministerial element to the authorisation process:

> "I recommended a double lock myself in relation to foreign policy and defence warrants. But in relation to police warrants, which are 70% of the whole and therefore represent 70% of those 2,300 warrants that the Home Secretary authorises every year, it seems to me that one could do without the politician or the Minister and go straight to the judicial commissioner."[331]

This suggestion would help to allay the concerns of those who believe that ministerial involvement in authorising all warrants may become unsustainable as the number of warrants continues to rise.

421. **The Committee is satisfied that a case has been made for having a 'double-lock' authorisation for targeted interception, targeted equipment interference, and bulk warrants.**

Judicial Review

422. A large number of witnesses questioned whether the intended "double-lock" system is reflected accurately in the wording of relevant clauses. The draft Bill specifies that when making the authorisation decision "the Judicial Commissioner must apply the same principles as would be applied by a court on an application for judicial review."[332]

423. The Committee received numerous submissions on the issue of judicial review principles and how the wording of these clauses affect the tests that the judicial commissioners will be applying when deciding whether to authorise a warrant. Many of the submissions raised concerns about the inclusion of judicial review principles for various reasons.[333]

331 Q 68 (David Anderson QC)

332 See Clauses 19(2), 90(2), 109(2), 123(2), 138(2), 155(2)

333 See, for example, written evidence from Peter White (IPB0004), Big Brother Watch (IPB0007), News Media Association (IPB0012), Giuseppe Sollazzo (IPB0032), Krishan Bhasin (IPB0034), the Chartered Institute of Legal Executives (IPB0041), Ms Susan Morgan (IPB0043), Dr Andrew Defty (IPB0050), Article 19 (IPB0052), the Bingham Centre for the Rule of Law (IPB0055), Dr Glyn Moody (IPB0057), Open Intelligence (IPB0066), Mr. Bernard Keenan, Dr. Orla Lynskey, Professor Andrew Murray (IPB0071), the Information Commissioner's Office (IPB0073), Amnesty International UK (IPB0074), BCS, The Chartered Institute for IT (IPB0075), techUK (IPB0088), Cian C Murphy and Natasha Simonsen (IPB0096), Chartered Institute of Library and Information Professionals (IPB0104), The Law Society (IPB0105), Open Rights Group (IPB0108), Center for Democracy & Technology (IPB0110), Dr Christian Heitsch (IPB0111), Facebook Inc., Google Inc., Microsoft Corp., Twitter Inc. and Yahoo Inc. (IPB0116), Privacy International (IPB0120), Human Rights Watch (IPB0123), Dr Julian Huppert (IPB0130), GreenNet (IPB0132), Bar Council (IPB0134), Equality and Human Rights Commission (IPB0136), McEvedys Solicitors & Attorneys Ltd (IPB0138), Liberty (IPB0143), BT (IPB0151) and Yahoo (IPB0155)

EMBARGOED until 09:30 on 11 February 2016

424. Some witnesses thought that the judicial review test was too narrow to allow the judge to make an authorisation based on the merits of the case. Article 19 wrote that:

> "the usual standard applied is Wednesbury unreasonableness, which means that the judge cannot disturb the Secretary of State's conclusions as to necessity and proportionality unless he or she is satisfied that the decision was so unreasonable that no reasonable person could have arrived at such a decision. This is an extraordinarily low threshold for the Secretary of State to have to meet, meaning that it is highly unlikely that a judge would ever reverse the Secretary of State's decision."[334]

This led to some concern from witnesses that the involvement of judicial commissioners in these authorisations would be a "rubber-stamping" exercise.

425. We also heard evidence from a panel of specialist lawyers who were largely in agreement about the effect of imposing judicial review rules. Matthew Ryder QC said "In a judicial review situation, the judge is essentially bound by decisions and assessments of facts that have been made by the Secretary of State".[335]

426. Others challenged this position, contending that the judicial review test provides for a thorough review based on the merits of the case. Dr Tom Hickman said,

> "the fact that the [judicial commissioners (JCs)] will be mandated to apply judicial review principles does not mean that they will apply a Wednesbury review. It is trite law that in human rights cases courts will decide for themselves whether a measure is necessary and proportionate and these are the judicial review principles that judges will surely adopt (e.g. *Miss Behavin' Ltd* [2007] 1 WLR 1420)."[336]

427. The Rt Hon Lord Judge and the Rt Hon Sir Stanley Burnton agreed with this assessment. Lord Judge said "Judicial review used to be Wednesbury unreasonable mad. We would call it Wednesbury unreasonable, meaning only an idiot could have reached this decision. Nowadays, judicial review is less stringent than that."[337] In the same vein, Sir Stanley Burnton said that "you can forget about Wednesbury unreasonableness in this context. Interestingly, proportionality and necessity are tests that we have imported from Europe, and the proponents of the Bill are clearly happy to adopt them in this context."[338]

428. In his oral evidence to the Committee, Paul Lincoln, Director, National Security (Office for Security and Counter-Terrorism) at the Home Office, said in relation to judicial authorisation of warrants: "The specifics here are that two things will be critical: first, that they decide in the first place that the action is rational and lawful; and, secondly, that it is necessary and proportionate. Those are exactly the same tests as the ones the Secretary of State will be looking at."[339] The Home Secretary in her evidence to the Committee said that the purpose of judicial review principles was to accord judges "a degree of flexibility as to how they approach particular cases depending on the impact on the individual of

EMBARGOED until 09:30 on 11 February 2016

334 Written evidence from Article 19 (IPB0052)
335 Q 190 (Matthew Ryder QC)
336 Written evidence from Dr Tom Hickman (IPB0039)
337 Q 53 (Lord Judge)
338 Q 53 (Sir Stanley Burnton)
339 Q 9 (Paul Lincoln, Home Office)

what it is they are looking at." The Home Secretary also made clear that "they are not re-taking the decision. They are looking to see whether the original decision was flawed."[340]

429. A further issue for the authorisation procedure as set out in the draft Bill is the absence of any adversarial process which is usually a feature of judicial review. As Matthew Ryder QC told the Committee:

> "normally in judicial review, there is an element of an adversarial process. In other words, the judge is assessing it with somebody making representations in relation to the other side. There will be no adversarial process built into this, the way it stands at the moment. You will have a judicial review, but no one putting forward the argument to the judge in a different situation. Now, that is not unheard of; you have that in other situations, but not in relation to a judicial review situation."[341]

430. Professor Christopher Forsyth mentioned the three grounds of procedural irregularity, irrationality and illegality as the basic principles of judicial review and in doing so highlighted that:

> "there is another consideration here that suggests that judicial review principles are, in a way, unsuitable or would have to be thought about a bit more carefully … Procedural irregularity is, of course, the principle that people should be heard and given the opportunity to make their case before a decision adverse to their interests is taken. That, of course, cannot happen in the kind of context that we are talking about … It means that a whole slice of judicial review principles has been discarded for the purposes of this exercise."[342]

431. In support of this argument, the News Media Association told us that "while the applicant can challenge a refusal, the oblivious media organisation, journalist or indeed any other potential subject affected, cannot contest the application, the grant of consent, or review of a refusal, or even make a retrospective complaint" owing to the ban on disclosure of the existence of these warrants.[343] This point is discussed in more detail at paras 539–556 which address issues relating to journalistic privilege.

432. As a result, some witnesses[344] suggested that the Bill should make provisions for there to be special counsels or advocates to the Judicial Commissioners in order to "enable arguments to be developed as to why a warrant request goes too far or is inadequately supported etc."[345]

433. **The Committee is satisfied with the wording in the Bill and believes that the judicial review principles will afford the Judicial Commissioners a degree of flexibility, as outlined by the Home Secretary.**

EMBARGOED until 09:30 on 11 February 2016

340 Q 273 (Theresa May MP)
341 Q 190 (Matthew Ryder QC)
342 Q 217 (Professor Christopher Forsyth)
343 Written evidence from the News Media Association (IPB0012)
344 For example, written evidence from the Bingham Centre for the Rule of Law (IPB0055) and Amnesty International UK (IPB0074)
345 Written evidence from Dr Tom Hickman (IPB0039)

Targeted Interception

434. Targeted interception warrants are subject to the new 'double-lock' procedure. Previously they have been authorised solely by the Secretary of State.

Modification of warrants

435. Clause 26 of the draft Bill sets out the process for modifying a targeted interception warrant. It distinguishes between a major modification which must be authorised by a minister or senior official, and a minor modification which can be made by the person to whom the warrant is addressed, or another senior person in that public authority. There is no requirement for either type of modification to be authorised by a Judicial Commissioner.

436. Witnesses expressed concerns about the modification process for targeted interception warrants and believe that it would undermine the 'double-lock' authorisation process introduced in the Bill.[346] The Open Rights Group wrote: "The Secretary of State and senior officials would have very broad powers to change names, premises, or even to add multiple names without requirement for judicial commissioner approval. Such major modifications to a warrant would appear to deserve a similar level of scrutiny as the original authorisations."[347]

437. The Home Secretary emphasised to the Committee that "the necessity and proportionality of a warrant against a particular individual will have been determined by the double-lock authorisation process. Anything that was in that order would not count as a modification. Anything that required a warrant against a particular individual would require the double-lock authorisation process."[348]

438. **The Committee believes that this response fails to recognise that a modification, as currently worded in the draft Bill, might include adding a whole new set of people or premises to an existing warrant. The warrant could therefore be changed in a substantial way without any judicial oversight.**

439. ***The Committee recommends that major modifications for targeted interception warrants, as defined in the draft Bill, should also be authorised by a Judicial Commissioner. (Recommendation 32)***

Authorising interception in Scottish psychiatric hospitals

440. The draft Bill sets out the authorisation procedures for interception in psychiatric hospitals in Clause 38. The Mental Welfare Commission for Scotland drew the Committee's attention to an issue regarding the existing statutory framework for interception in Scottish psychiatric hospitals:

> "We are concerned that this does not properly take account of the statutory framework within which security measures, including interception of postal

346 For example, written evidence from Big Brother Watch (IPB0007), Dr Tom Hickman (IPB0039), Amnesty International UK (IPB0074), Open Rights Group (IPB0108), Privacy International (IPB0120), the Law Society of Scotland (IPB0128), Dr Julian Huppert (IPB0130), JUSTICE (IPB0148) and Yahoo (IPB0155)

347 Written evidence from Open Rights Group (IPB0108)

348 Q 275 (Theresa May MP)

EMBARGOED until 09:30 on 11 February 2016

> correspondence and telephone calls, operate in Scottish psychiatric hospitals. This is set out in sections 281 to 286 of the Mental Health (Care and Treatment) (Scotland) Act 2003."[349]

441. The Law Society of Scotland also expressed concern regarding this apparent oversight and suggested "that the provisions of Clause 38 should expressly provide that any action which is authorised under the 2003 Act is lawful."[350]

442. Furthermore, both witnesses argued that the Government should avoid creating two overlapping regimes. The Mental Welfare Commission for Scotland said:

> "unless there is some clear justification, the Bill should not add another route to authorising interception in a psychiatric hospital when there is already a statutory regime covering this. That is likely to create confusion as to how the two regimes interact.
>
> The approach of the 2003 Act is preferable, as much of the detail is in secondary legislation rather than Ministerial direction, so is subject to a greater degree of Parliamentary scrutiny. If there is concern that there are gaps in the framework of the 2003 Act, these gaps should be addressed within that framework, rather than create two overlapping regimes."[351]

443. **The omission of a reference to the Mental Health (Care and Treatment) (Scotland) Act appears to us to be an oversight, which we agree could lead to the creation of conflicting authorisation regimes for the use of interception in psychiatric hospitals in Scotland.** ***The Committee recommends that this apparent oversight be addressed in the revised Bill. (Recommendation 33)***

444. ***The Committee was provided with a table of investigatory powers in other legislation by the Home Office.***[352] ***As the Mental Health (Care and Treatment) (Scotland) Act 2003 was missed off this table, we are concerned that there may be other omissions. We recommend that the Home Office should further review its list of investigatory powers in other legislation to ensure that nothing else has been overlooked. (Recommendation 34)***

Targeted Equipment Interference

445. The draft Bill also brings targeted equipment interference warrants under the 'double-lock' authorisation regime.

Differences in authorisation and modification for law enforcement and intelligence agencies

446. The draft Bill differentiates between law enforcement and intelligence agencies in respect of the process for both authorising and modifying targeted equipment interference warrants. Clause 84 relates to warrants applied for by the security and intelligence agencies and says that they must be authorised by the Secretary of State and a Judicial Commissioner. In comparison, Clause 89 provides for law enforcement chiefs and a

349 Written evidence from the Mental Welfare Commission for Scotland (IPB0029)
350 Written evidence from the Law Society of Scotland (IPB0128)
351 Written evidence from the Mental Welfare Commission for Scotland (IPB0029)
352 Written evidence from the Home Office (IPB0159)

EMBARGOED until 09.00 on 11 February 2016

Judicial Commissioner to authorise equipment interference warrants for law enforcement officers.

447. Additionally, Clause 96 sets out the procedure for modifying warrants and says that modifications for law enforcement warrants must be authorised by a Judicial Commissioner but this requirement is not present for the intelligence agencies.

448. The Interception of Communications Commissioner's Office said that "the different procedures are confusing and it is not clear on what basis they are justified"[353] and the Information Commissioner's Office recommended that "there should be a consistent and appropriately robust approach adopted."[354]

449. The Home Secretary explained the reasoning for this approach:

> "With regard to modifications to the different warrants from either the agencies or from law enforcement, modifications to the agency warrants require approval from the warrant issuer, which is the Secretary of State or designated official, so that they are being looked at independently from the agency. Where there is a modification to law enforcement … the issuing authority is the internal law enforcement chief. To give the independence, that is why we have instructed that the Judicial Commissioner should also authorise modifications for law enforcement equipment interference warrants. It is about getting that degree of independence but it can be achieved in different ways."[355]

450. **The Committee believes that the differential approach to authorisations and modifications for targeted equipment interference warrants applied to the security and intelligence agencies and law enforcement agencies is confusing and unjustified.** ***We therefore recommend that the approach to targeted equipment interference warrants should be standardised and that all modifications should be subject to judicial authorisation. (Recommendation 35)***

Discrepancy between draft Bill and Code of Practice

451. In relation to both targeted and bulk equipment interference, the Home Office published a draft Code of Practice alongside the draft Bill.[356] Witnesses suggested that there was some discrepancy between the safeguards set out in the Code of Practice and the actual requirements in the draft Bill. Open Intelligence explained:

> "The requirements set out for both targeted interference in Clause 93 and bulk interference in Clause 140 fall short of the guidelines set out for applications for warrants in 4.6 of the Draft Equipment Interference Code of Practice [DECIP]. Clauses 93 and 140 should also set out as in 4.6 of the DEICP requirements to contain the nature and extent of the proposed interference, details of potential collateral intrusion, what the operation is expected to deliver, details of offences suspected, action necessary to install, modify or remove software.

353 Written evidence from the Interception of Communications Commissioner's Office (IPB0101)
354 Written evidence from the Information Commissioner's Office (IPB0073)
355 Q 276 (Theresa May MP)
356 Home Office, *Equipment Interference Draft Code of Practice*, November 2015

EMBARGOED until 09:30 on 11 February 2016

In the case of bulk equipment interference an assessment of potential damage and vulnerabilities that may be incurred should be included."[357]

452. **The Committee is satisfied that the safeguards for equipment interference are adequately set out in the Code of Practice and do not need to also be reflected on the face of the Bill.**

Issues common to targeted interception and targeted equipment interference warrants

Urgent Warrants

453. The draft Bill makes provisions for the Secretary of State to authorise a targeted interception or targeted equipment interference warrant without judicial authorisation if the minister considers that there is an "urgent need to issue it".[358] The warrant must then be reviewed by a Judicial Commissioner within five working days. It ceases to have effect if it is not authorised by the Judicial Commissioner during that period. Witnesses raised concerns about this provision, in particular with regards to the protection of human rights, the time allowed for the Judicial Commissioner to review the warrant, and the lack of a definition of 'urgent'.

454. The News Media Association suggested that the process for urgent warrants allows "the 'so called double lock' to be bypassed, even where it applies, so that the powers can be used and damage done long before the review deadline and any possible revoke."[359] Access Now said that, as a result, "this process fails to provide sufficient human rights protections or adequate oversight."[360]

455. Furthermore, numerous submissions contended that the five day review period for urgent warrants was excessive and unjustified.[361] The Bar Council told the Committee that "High Court Judges frequently listen to and grant orders made on urgent application. Provided sufficient Commissioners are appointed there is no reason why they would not be at least as available to make a decision as the Secretary of State."[362]

456. **While the Committee accepts that there will be some exceptionally urgent circumstances in which a warrant will need to be authorised immediately, it is not clear why the period for the Judicial Commissioner to review and authorise the warrant should be as long as five working days.**

457. Witnesses emphasised that "it is easy to see how [the five day] provision may become a loophole ripe for excess and/or abuse".[363] ***The Committee therefore recommends that the period in which urgent warrants must be reviewed by a Judicial Commissioner should be shortened significantly. We suggest that they must be reviewed within 24 hours of their signature by the Secretary of State. (Recommendation 36)***

357 Written evidence from Open Intelligence (IPB0066). See, also, written evidence from Electronic Frontier Foundation (IPB0119) and Liberty (IPB0143).
358 See Clauses 20 and 91
359 Written evidence from News Media Association (IPB0012)
360 Written evidence from Access Now et al. (IPB0109)
361 For example, written evidence from the Bingham Centre for the Rule of Law (IPB0055), Amnesty International UK (IPB0074), Privacy International (IPB0120) and the Bar Council (IPB0134) and Q 175 (Baroness Jones of Moulescoomb)
362 Written evidence from the Bar Council (IPB0134)
363 Written evidence from Amnesty International UK (IPB0074)

EMBARGOED until 09.30 on 11 February 2016

458. Others focused on the lack of definition of the word 'urgent'. As a result the urgency procedure could "be interpreted to encompass a wide array of circumstances".[364] Witnesses suggested that "clarity on this term—which other countries may seek to emulate and even abuse—is important."[365] **We agree that greater clarity on the term "urgent" is required.**

459. The Committee received a letter from John Hayes MP, Minister of State for Security, who sought to clarify this issue. He wrote, "In practice, a warrant is only treated as urgent if there is an immediate and limited window of opportunity to achieve the aim of the warrant. Typically the urgency provision is used in relation to a fleeting intelligence or evidence-gathering opportunity or an imminent threat to life or serious harm."[366]

460. ***The Committee recommends the inclusion of a definition of the word "urgent" for the purposes of authorising urgent warrants. (Recommendation 37)***

Thematic Warrants

461. The Committee heard some concerns about the potentially broad subject matter of targeted interception and targeted equipment interference warrants. Clause 13(2) relating to targeted interception warrants states that "a targeted interception warrant may relate to a group of persons who share a common purpose or who carry on, or may carry on, a particular activity". Clause 83 relating to targeted equipment interference warrants is similarly broad. It provides that such warrants may relate to "equipment in a particular location", "equipment in more than one location", or "equipment that is being, or may be being used, for the purposes of a particular activity or activities of a particular description."

462. There is therefore the potential for these clauses to be interpreted as authorising 'thematic warrants', as Matthew Ryder QC suggested, "warrants based not on the identity of known individuals, or the identity of a known group of individuals, but on a theme relating to general activity by persons unknown (e.g. all persons within a city who may be committing activity of a certain description). Such an interpretation transforms what are presented as domestic 'targeted' interception warrants into warrants that permit general surveillance in the hope of determining who, amongst potentially millions of people, might be engaged in the activity in question."[367]

463. Witnesses expressed concerns about the contexts in which these powers could be deployed. The Network for Police Monitoring highlighted the possibility that "in the context of protest policing, this extends the use of surveillance activities to any individual associated with a protest groups… Not only does the surveillance extend to individuals themselves engaging in (possibly low-level) criminal activity, it arbitrarily extends it to all individuals believed to share a 'common purpose' with them."[368]

464. The Center for Democracy and Technology went further and suggested that:

> "such language does not, by its terms, exclude the possibility that everyone who belongs to a certain trade union, political party or book club; visits a certain shop; attends (or has friends or family members who attend) a certain

364 Written evidence from Privacy International (IPB0120)
365 Written evidence from Facebook Inc., Google Inc., Microsoft Corp., Twitter Inc. and Yahoo Inc. (IPB0116)
366 Written evidence from the Home Office (IPB0159)
367 Written evidence from Matthew Ryder QC (IPB0142)
368 Written evidence from the Network for Police Monitoring (Netpol) (IPB0087)

EMBARGOED until 09:30 on 11 February 2016

house of worship; subscribes to a certain publication; participates in a lawful and peaceful demonstration; celebrates or may celebrate a certain religious or national holiday; or uses a particular e-mail or instant messaging service may experience very serious privacy intrusions pursuant to a 'targeted' warrant in a manner that cannot reasonably be regarded as foreseeable."[369]

465. Additionally, some witnesses suggested that the scope of these warrants as proposed in the draft Bill could be in violation of Article 8, especially in light of the ECtHR judgement in *Zakharov v Russia*. Liberty told us that, where the ECtHR "found Russia's interception scheme in violation of Article 8 of the Convention, the Court cited the fact that Russian 'courts sometimes grant interception authorisations which do not mention a specific person or telephone number to be tapped, but authorise interception of all telephone communications in the area where a criminal offence has been committed.' While thematic warrants do not relate to geographical location, they are sufficiently broad to violate Article 8."[370]

466. The Secretary of State explained in her evidence to the Committee that "it will not be possible to use a thematic warrant against a very large group of people. The purpose of a thematic warrant is, for example, circumstances in which perhaps somebody has been kidnapped or there is a threat to life, where only certain information is available, and it is necessary because of the pace at which something is developing to identify the group of people who are involved with that particular criminal activity as being within the thematic warant."[371]

467. The Home Secretary's statement is helpful in that it clarifies some of the legitimate uses for such a warrant. But she did not acknowledge that the wording in the draft Bill would allow a much broader interpretation which could lead to some of the activities identified by the Center for Democracy and Technology. **The Committee agrees that the current wording of the provisions for targeted interception and targeted equipment interference warrants is too broad.**

468. ***The Committee recommends that the language of the Bill be amended so that targeted interception and targeted equipment interference warrants cannot be used as a way to issue thematic warrants concerning a very large number of people. (Recommendation 38)***

Communications Data and Internet Connection Records

Authorisation for Targeted Communications Data and ICRs

469. Communications Data is considered by the draft Bill to be less intrusive than the other investigatory powers. As a result, the authorisation process is less burdensome and is not subject to the 'double-lock'. An investigator who wants access to communications data, including ICRs, must consult with a Single Point of Contact (SPoC) who can advise the applicant on relevant aspects of the application before it is made to a senior designated officer. It is then up to the senior designated officer to decide whether to authorise the request. Requests from a local authority (who may apply for communications data but

369 Written evidence from the Center for Democracy & Technology (IPB0110)
370 Written evidence from Liberty (IPB0143)
371 Q 276 (Theresa May MP)

EMBARGOED until 09:30 on 11 February 2016

not ICRs) are sent to a magistrate for authorisation instead of a senior designated officer, and requests to determine a journalistic source are sent to a Judicial Commissioner for authorisation.

470. As has been detailed above in the Capabilities chapter, the less intrusive nature of data communications was called into question by a number of witnesses. Accordingly, many are concerned that the authorisation process for communications data continues to be at a lower level than other investigatory powers and have suggested submitting applications for communications data to the 'double-lock' procedure.[372] Scottish PEN said:

> "Requiring public bodies to seek approval through a communications data acquisition notice and not a warrant signed by a judge removes a much-needed level of oversight to ensure that they are independently judged to be acting in a "necessary and proportionate" manner. While the designated person is required to be independent from the investigative team requesting the notice, the fact that they are representing the same body raises key questions as to whether this amounts to independent scrutiny."[373]

471. The Committee also received a number of submissions commending the existing process for authorisation which the draft Bill replicates. EE told us "the use of Single Points of Contacts (SPOCs) is a strong, transparent, and stringent process. A SPoC must always be engaged for the acquisition of CD and is specially trained and accredited in the use of CD and will advise upon the appropriate use of all available CD"[374] and LINX welcomed "the continued commitment to oversight by Single Points of Contact, which has been one of the more successful innovations introduced in the implementation of RIPA."[375]

472. Additionally, the Committee was able to visit the Metropolitan Police SPoCs and ask them questions about the work they do. The Committee found this helpful in understanding the process and were impressed by the knowledge and commitment of the SPoCs.

473. Given the high number of requests for communications data made each day, the Committee accepts that it would not be feasible to require judicial authorisation for all of them. David Anderson QC in his oral evidence[376] to the Committee referred to some examples he suggested in *A Question of Trust* which might benefit from an extra layer of authorisation. These were:

- "communications data for the purpose of determining *matters that are privileged or confidential*"
- Communications data relating "to *persons who handle privileged or confidential information* (doctors, lawyers, journalists, MP, etc.)"

EMBARGOED until 09:30 on 11 February 2016

372 For example, written evidence from Dr Paul Bernal (IPB0018), Article 19 (IPB0052), Open Intelligence (IPB0066), Dr Richard Clayton (IPB0085), Chartered Institute of Library Information Professionals (IPB0104), Open Rights Group (IPB0108), Center for Democracy & Technology (IPB0110), Privacy International (IPB0120), Human Rights Watch (IPB0123), Liberty (IPB0143) and Virgin Media (IPB0160)

373 Written evidence from Scottish PEN (IPB0076)

374 Written evidence from EE (IPB0139)

375 Written evidence from LINX (IPB0097)

376 Q 72 (David Anderson QC)

- "Where a *novel or contentious request* is made for communications data."[377]

474. ***The Committee is satisfied that the proposed authorisation process for communications data is appropriate but recommends that extra protections for privileged and confidential communications should be applied in the same way as is proposed for journalists in Clause 61. (Recommendation 39)***

Local Authority authorisation

475. The draft Bill maintains the current authorisation procedure for local authorities, which was introduced in 2012, requiring them to seek authorisation from a magistrate for access to communications data. The draft Bill also precludes local authority access to ICRs.

476. The LGA and NAFN told us that "in practice the process of seeking judicial approval can be slow and inefficient" and that this "acts as a deterrent to councils seeking access to communications data when there is a legitimate basis for them to do so."[378] The IOCCO has also previously commented that 40% of the public authorities that have powers to acquire communications data have never used their powers.[379]

477. The LGA and NAFN suggested that "councils are able to apply for and be granted magistrates approval electronically" and that "Central government should also consider the case for routing all such applications through a small number of magistrates' courts with direct links to the National Anti-Fraud Network. By creating centres of expertise, this would ensure that this safeguard is applied consistently and robustly."[380] These sentiments are echoed in the submission by Trading Standards North West.[381]

478. **The Committee understands the value of local authorities being able to access communications data in limited circumstances and is content with the proposed authorisation process.**

Serious Fraud Office authorisation

479. The Committee has also received a submission from the Serious Fraud Office setting out some concerns regarding Clause 63(5) of the draft Bill which gives the Secretary of State authority to direct that agencies enter collaboration agreements. They are concerned that this will be used to require them to share a SPoC with other public authorities. They told us that "this is not the preferred authorisation process for the SFO because of the need to protect confidentiality and operational security of our investigations."[382]

EMBARGOED until 09:30 on 11 February 2016

377 David Anderson QC, *A Question of Trust: Report of the Investigatory Powers Review*, 2015, Executive summary, paras 25–27

378 Written evidence from the Local Government Association (LGA), National Anti-Fraud Network (NAFN), Chartered Trading Standards Institute and Association of Chief Trading Standards Officers (IPB0051)

379 The Interception of Communications Commissioner, *Report of the Interception of Communications Commissioner* ,March 2015, Para 7.10

380 Written evidence from the Local Government Association (LGA), National Anti-Fraud Network (NAFN), Chartered Trading Standards Institute and Association of Chief Trading Standards Officers (IPB0051)

381 Written evidence from Trading Standards North West (IPB0092)

382 Written evidence from the Serious Fraud Office (IPB0153)

Emergency authorisation procedures

480. In the interests of national security, or if there is an imminent threat to life, Clauses 47(2) and 60(2) allow for some changes to the communications data authorisation process. They remove the requirement for the designated person to be independent from the investigation when approving the acquisition or disclosure of communications data and they remove the requirement for the public authority to consult with a SPoC when acquiring communications data. The Interception of Communications Commissioner's Office questioned the need for the provision in Clause 47 and said that it "dilutes the independence safeguard recently introduced into the March 2015 Communications Data Code of Practice (as a consequence of the Digital Rights Ireland case which resulted in a ruling by the ECJ)."[383]

481. Virgin Media expressed some concerns about bypassing SPoCs:

> "This is not necessary or good practice. We believe that emergencies can be dealt with through LEA co-operation agreements to share the use of SPOCs to ensure 24x7 cover. If a police officer is able to bypass a SPOC, then all the controls set up to: (a) ensure an appropriate request is made in the manner most likely to result in disclosure of relevant data; and (b) ensure data is only disclosed to authorised individuals; will also be bypassed. We believe this is a very important safeguard, and its removal creates an unnecessary security risk."[384]

482. ***The Committee recommends the removal of emergency procedures for communications data so that the Single Point of Contact process can never be bypassed. (Recommendation 40)***

Powers to modify Clause 54 and Schedule 4

483. The Committee is grateful to the House of Lords Delegated Powers and Regulatory Reform Committee for providing a detailed memorandum on the various delegated powers within the draft Bill. As highlighted in their memorandum:

> "Clause 55(1) confers power on the Secretary of State by regulations to amend Clause 54 and Schedule 4. The power includes a power to add or remove a public authority from the list in Schedule 4 and to modify an entry about the rank etc. of a designated senior officer. The regulations can also impose or remove restrictions on the authorisations which a particular kind of designated senior officer may give, and impose or remove restrictions on the circumstances or purposes for which authorisations may be given."[385]

484. The DPRRC accepted the justification for this power and welcomed the enhanced affirmative procedure that the draft Bill applies to it. This is in contrast to the ordinary affirmative procedure that was applied under RIPA.

383 Written evidence from the Interception of Communications Commissioner's Office (IPB0101)
384 Written evidence from Virgin Media (IPB0160)
385 Memorandum from the House of Lords Select Committee on Delegated Powers and Regulatory Reform (see Appendix 3)

EMBARGOED until 09:30 on 11 February 2016

485. **The Committee agrees with the conclusions of the DPRRC on the enhanced affirmative procedure for amendments to Clause 54 and Schedule 4. We join them in welcoming the strengthening of scrutiny procedures in this area of the draft Bill.**

486. The DPRRC pointed out that "Clause 56(1) sets out circumstances in which the negative rather than the enhanced affirmative procedure will apply to regulations under Clause 55(1). These are where the regulations only have effect:

- to remove a public authority from the list in Column 1 of the table in Schedule 4 and make consequential modifications; or
- to modify the list of ranks, offices etc. that must be held by a designated senior officer as set out in Column 2 of that table."[386]

487. While the DPRRC was satisfied that the negative procedure was appropriate in relation to the first bullet point, they were not "convinced that the negative procedure affords the appropriate level of scrutiny in all cases where it is proposed to modify Column 2 of the table in Schedule 4. We consider the requirement for an authorisation to be given at a high level within an organisation offers an important protection against an inappropriate use of the powers conferred by Part 3. **Accordingly, we think that any regulations modifying Column 2 which have the effect of lowering the level at which an authorisation has to be given should be subject to at least the affirmative procedure.**"[387]

488. The same conclusion was reached regarding Clause 57(4) which confers a power on the Secretary of State by regulations to amend subsection (2) and is subject to the negative procedure.

489. ***The Committee agrees with the recommendation of the DPRRC on modifications to the list of ranks and offices which must be held by a designated senior officer. We recommend that Clause 56(1) and Clause 57(4) should be amended accordingly. (Recommendation 41)***

Bulk powers warrants

Necessity and Proportionality test

490. Bulk interception warrants, bulk acquisition warrants, and bulk equipment interference warrants are all subject to the 'double-lock' authorisation process.

491. Submissions regarding authorisation for these bulk powers focused on the difficulty that the Judicial Commissioners could have when assessing the necessity and proportionality of the proposed actions.[388] As JUSTICE explained, "the breadth of application of some of the powers concerned may make it particularly difficult to assess necessity and proportionality in any meaningful way, undermining the ability of any

EMBARGOED until 09:30 on 11 February 2016

386 *Ibid.*
387 *Ibid.*
388 For example written evidence from BCS, The Chartered Institute for IT (IPB0075), Global Network Initiative (IPB0080), The Institute for Human Rights and Business (IPB0094), Access Now et al. (IPB0109), Dr Christian Heitsch (IPB0111), Privacy International (IPB0120), Human Rights Watch (IPB0123), Bar Council (IPB0134), McEvedys Solicitors and Attorneys Ltd (IPB0138), and JUSTICE (IPB0148)

authorising body, including a Judicial Commissioner to act as a significant safeguard against abuse."[389]

492. We note that judicial commissioners will have access to all the material that the Secretary of State will have when making their decision and will be able to question the applicants from the security and intelligence agencies on the details to satisfy their understanding before making a judgement.

493. **Subject to the views of the Intelligence and Security Committee regarding bulk powers, we are confident that the Judicial Commissioners would be able to assess the necessity and proportionality criteria in relation to bulk warrants.**

Bulk personal datasets

494. Part 7 of the draft Bill sets out provisions relating to the acquisition, examination and retention on bulk personal datasets. It allows the acquisition of specific datasets, as well as classes of datasets, when they have been authorised under the 'double-lock' procedure. Clause 154(6) also allows a warrant to authorise the obtaining, retention and examination of a dataset which does not yet exist (this is termed a "replacement dataset").

495. As well as concerns about the types of datasets to which the Agencies will have access, witnesses also criticised the authorisation process for class BPDs. Dr Tom Hickman said: "class authorisation is inadequate. It is difficult to understand why the datasets cannot be listed expressly in any warrants so that there is clear judicial sight of what data sets are being held and used. If there is to be proper democratic licence for these activities, there needs, at a minimum, to be greater visibility as to the breadth of the power, and full judicial approval."[390]

496. Concerns were also raised regarding replacement datasets. Eric King suggested that "Bulk Personal Dataset warrants must describe specific individual datasets. Provisions in warrantry as per section 152(6) to allow warrants to authorise the obtaining, retention and examination of "replacement datasets" that do not exist at the time of the issue of the warrant should be removed."[391]

497. ***The Committee recommends that authorisations for bulk personal datasets should be required to be specific and provisions for class authorisations should be removed from the Bill. The provision relating to replacement datasets (Clause 154(6)) should also be removed. (Recommendation 42)***

Technical Capability notices and National Security notices

Process for issuing these notices

498. The draft Bill enables the Secretary of State to serve these notices on a communications service provider in order to assist intelligence agencies or law enforcement in their work.[392]

389 JUSTICE (IPB0148)
390 Written evidence from Dr Tom Hickman (IPB0039)
391 Written evidence from Mr Eric King (IPB0106)
392 See Clauses 188 and 189

EMBARGOED until 09:30 on 11 February 2016

499. Submissions from Facebook Inc., Google Inc., Microsoft Corp., Twitter Inc., Yahoo Inc. and Virgin Media questioned why these notices were not subject to judicial authorisation before being served on communications service providers.[393] Human Rights Watch made the case for enhanced authorisation processes for these notices: "These broadly and ill-defined powers raise novel legal and technical questions that should be subject to substantive as well as procedural prior review by an independent judge, along with scrutiny by other oversight bodies."[394]

500. EE, another communications service provider, welcomed the process set out in the draft Bill for the issuing of these notices:

> "we welcome the fact that before a Notice can be served upon a telecommunications operator (in order to develop a technical capability to support EI), the Secretary of State must first consult with the telecommunications operator to assess, amongst other things, proportionality, technical feasibility, cost and impact on the network and their customers. Following this process, if after a Notice has been served, a telecommunications operator still has concerns with the content of that Notice, the Notice can be referred back to the Secretary of State for review, who has a duty to consult with the Technical Advisory Board and the Investigatory Powers Commission (IPC)."[395]

501. The Home Secretary, when asked why the 'double-lock' procedure will not be applied to National Security and Technical Capability notices, explained that "the double-lock authorisation is there where there are processes that are intrusive into an individual. When you look at the technical capability and national security notices, those are of a different order. They are not about that question of the intrusion that is taking place into an individual."[396]

502. **The Committee accepts that National Security and Technical Capability notices are different in scope and intrusion to the types of warrants that will need to be authorised by a Judicial Commissioner. We are therefore content that these notices should be issued by the Secretary of State without reference to a Judicial Commissioner.**

Data sharing and Extraterritoriality

503. The draft Bill provides powers for the UK to share information with overseas intelligence and law enforcement agencies, as well as asserting extraterritoriality so that information can be obtained from companies based outside of the UK.

504. The Committee is aware that the Government has been working on implementing the recommendations made by Sir Nigel Sheinwald's Report. These included:

- Improving government-to-government cooperation
- Reforming the existing US/UK Mutual Legal Assistance Treaty (MLAT) so that issues around timeliness of information sharing can be resolved

393 Written evidence from Facebook Inc., Google Inc., Microsoft Corp., Twitter Inc. and Yahoo Inc (IPB0116) and Virgin Media (IPB0160)
394 Written evidence from Human Rights Watch (IPB0123)
395 Written evidence from EE (IPB0139)
396 Q 277 (Theresa May MP)

EMBARGOED until 09:30 on 11 February 2016

- Building a new international framework for intelligence sharing
- Improving transparency around the number and nature of requests to overseas and domestic CSPs.[397]

505. The Home Secretary wrote to the Committee to provide an update on the Government's work in this area, saying "We have continued to engage in preliminary discussions with international partners on how such an agreement might operate in principle, based on strong, human rights-compliant domestic regulatory frameworks. In the discussions I have held, there is a consensus about the broad principles behind an agreement, but we are not yet at the stage of any formal negotiations."[398]

Safeguards for data sharing overseas

506. A number of witnesses criticised the draft Bill for lacking detail about conditions for sharing information with overseas authorities. Taking as an example Clause 39 which deals with interception in accordance with overseas requests, Amnesty International UK wrote that "it is an extremely broad enabling provision that cannot begin to be sufficiently clear to satisfy the UK's human rights obligations in this field. It also leaves it open to the Secretary of State to make further Regulations as to conditions to be met for such sharing, without indicating what those might be."[399]

507. Other witnesses raised concerns about the lower level of safeguards that apply to sharing data overseas.[400] Privacy International said:

> "Except for the provisions regulating Mutual Assistance Warrants (that apply only to interception of communications) there is no mention in the IP Bill of the grounds, limits and authorisations required for sharing data obtained through surveillance. In this respect the IP Bill fails to resolve one of the most controversial and concerning practices of UK intelligence agencies, namely receiving and sharing acquired data in ways that are unregulated and may have the effect of circumventing applicable safeguards (notably under the Five Eyes arrangements). If confirmed, this would leave a significant loophole in the new regime regulating the use and oversight of investigatory powers, resulting in significant risks of abuse."[401]

508. Amnesty International UK and Privacy International also pointed to a lack of any provisions in the draft Bill regulating the receipt by the UK of material obtained through interception by overseas agencies. Amnesty International UK said that: "Schedule 6 provides at 2(2) a bare statement that Codes of Practice will cover the process for overseas requests and handling data received from them. Not only is this a wholly inadequate provision given the scale of what occurs, it makes no mention whatsoever of communications material received otherwise than through a specific request."[402]

397 Cabinet Office, *Summary of the Work of the Prime Minister's Special Envoy on Intelligence and Law Enforcement Data Sharing—Sir Nigel Sheinwald*, 25 June 2015
398 Written evidence from Theresa May MP (IPB0165)
399 Written evidence from Amnesty International UK (IPB0074)
400 See, for example, written evidence from Amnesty International UK (IPB074), Mr Eric King (IPB0106), Open Rights Group (IPB0108) and the Equality and Human Rights Commission (IPB0136)
401 Written evidence from Privacy International (IPB0120)
402 Written evidence from Amnesty International UK (IPB0074)

EMBARGOED until 09:30 on 11 February 2016

509. The Home Secretary explained that "before intercept material is shared with an overseas authority, the issuing authority sharing the material must be satisfied that they have appropriate handling arrangements in place to protect the material, equivalent to those that apply under Clause 40. Those might not be exactly mirrored; they might not be absolutely the same; but they are equivalent, so they give the same degree of appropriate handling arrangements."[403]

510. **The Committee believes that leaving the decision regarding the propriety of sharing intercept material with an overseas authority to the appropriate issuing authority is not a strong enough safeguard**.

511. ***The Committee would like to see more safeguards for the sharing of intelligence with overseas agencies on the face of the Bill. These should address concerns about potential human rights violations in other countries that information can be shared with. (Recommendation 43)***

512. ***The Committee also recommends that the Bill should make it illegal for UK bodies to ask overseas agencies to undertake intrusion which they have not been authorised to undertake themselves. (Recommendation 44)***

Dangers and difficulties of asserting extraterritoriality

513. The Committee has received a large volume of evidence regarding the potential difficulties of asserting extraterritoriality when making demands on communications service providers not based within the UK.

514. Apple Inc. told us that "there will remain a proportion of service providers which will never assist British law enforcement regardless of threatened sanction because they are underground or in jurisdictions unfriendly to British interests. It is to these providers that dangerous people will gravitate."[404] Added to this, Facebook et al. raised the issue that "unilateral assertions of extraterritorial jurisdiction will create conflicting legal obligations for overseas providers who are subject to legal obligations elsewhere."[405] BT suggested that "the introduction of judicial authorisation may persuade some overseas CSPs of the legitimacy of requests for interception."[406]

515. Concerns were also expressed about the precedent that this legislation might then set for other countries.[407] The Interception of Communications Commissioner's Office told us that "both UK and overseas businesses may be impacted by other countries following in the footsteps of the UK by adopting similar (but possibly not democratically controlled) investigatory powers regimes, particularly because the UK plays such a leading role in the global digital economy."[408]

516. Above all, in respect of extraterritoriality, there appear to be some inconsistencies in the safeguards against unreasonable warrants, the enforceability of different powers, and

403 Q 278 (Theresa May MP)
404 Written evidence from Apple Inc. and Apple Distribution International (IPB0093)
405 Written evidence from Facebook Inc., Google Inc., Microsoft Corp., Twitter Inc. and Yahoo Inc. (IPB0116). See also written evidence from Professor Andrew Woods (IPB0114)
406 Written evidence from BT (IPB0151)
407 For example, written evidence from Ms Susan Morgan (IPB0043), Global Network Initiative (IPB0080), techUK (IPB0088), Apple Inc. and Apple Distribution International (IPB0093), the Interception of Communications Commissioner's Office (IPB0101), Facebook Inc., Google Inc., Microsoft Corp., Twitter Inc. and Yahoo Inc. (IPB0116), Privacy International (IPB0120), Human Rights Watch (IPB0123) Liberty (IPB0143), Yahoo (IPB0155)
408 Written evidence from the Interception of Communications Commissioner's Office (IPB0101)

EMBARGOED until 09.30 on 11 February 2016

the circumstances in which the Secretary of State is obliged to consult with CSPs. Yahoo's submission summarised these variations in a single table, reproduced here.[409]

Table 2: Extraterritorial jurisdiction powers in the draft Bill

Provision	ETJ applies	Reasonable-ness test	Conflict of laws defence	Enforce-able against overseas CSP	International mutual assistance framework (within scope)	Obligation on SoS to consult CSP
Targeted interception Clause 29(4)	Yes	Yes Clause 31(5)	Yes Clause 31(5)	Yes Clause 31(8)	Yes	No
Targeted acquisition of comms data Clause 69	Yes	Yes Clause 69(4)	Yes Clause 69(4)	Yes Clause 50(4)	Yes	No
Mandatory data retention Clause 79	Yes	Partial[410]	No[411]	No	No	Yes Clause 72(2)
Targeted EI Clause 99(3)	Yes	Yes Clause 102(6)	No[412]	No	No	No
Bulk interception Clause 116(3)	Yes	Yes Clause 116(5)	Yes Clause 116(5)	Yes Clause 116(5)	No	Yes Clause 108(2)
Bulk acquisition of comms data Clause 130(3)	Yes	Yes Clause 130(5)	Yes Clause 130(5)	Ambiguous[413]	No	No
Bulk EI Clause 145(3)	Yes	Yes Clause 145(4)	No[414]	No	No	No
Bulk personal data sets Clause 150	No	-	-	-	-	-
Technical capability notice Clause 189	Yes	Partial[415]	No	Partial[416]	-	Yes Clause 190(2)

Source: Yahoo

409 Written evidence from Yahoo (IPB0155)
410 There's no explicit reasonableness test in this section but Clause 72(1) cover some of this ground.
411 Confusing as there is no explicit offence for failure to comply.
412 Confusing as there is no explicit offence for failure to comply.
413 Clause 130(6) could be aimed at UK CSPs only or also include local subsidiaries of overseas CSPs.
414 Confusing as there is no explicit offence for failure to comply.
415 Clause 130(3) is limited to technical feasibility and cost, not broader "reasonably practicable" test as in Clause 31.
416 If the notice relates to an enforceable power, then the notice is also enforceable—see Clause 190(10) and 190(11).

EMBARGOED until 09:30 on 11 February 2016

517. While the Committee is grateful for the written evidence it received from Facebook, Google, Microsoft, Twitter, Yahoo and Apple, we were disappointed that all refused to appear before the Committee to answer oral questions. Without this opportunity to cross-examine some of the strong opinions voiced in their written submissions, the Committee finds it difficult to come to a settled view on these issues. It is also difficult to form a view on claims made in some submissions that these extraterritorial elements of the draft Bill will be unenforceable.[417]

518. ***We recommend that the Government should give more careful consideration to the consequences of enforcing extraterritoriality. The Government should re-double its efforts to implement Sir Nigel Sheinwald's recommendations. (Recommendation 45)***

Privileged communications

Legal Professional Privilege

519. A number of witnesses expressed concerns as to the potential impact of the draft Bill on legal professional and journalistic privilege and the surveillance of Parliamentarians.[418]

520. Legal professional privilege ("LPP") is the right of a client to have "private communication with a lawyer, to obtain legal advice [or for the private provision of] advice and assistance in the course of litigation, whether active or potential".[419] There are no substantive provisions on the face of the draft Bill providing how LPP will apply when a warrant provides for the interception of communications which include those between a lawyer and his or her client. The only specific reference to legally privileged information is in Schedule 6 which requires the Secretary of State to make one or more codes of practice about the exercise of functions conferred by the draft Bill. Schedule 6, paragraph 4 provides that a code of practice about the obtaining or holding of communications data by virtue of Part 3 must include provision about "particular considerations applicable to any data which relates to a member of a profession which routinely holds legally privileged information or relevant confidential information". The draft Bill does not, however, state how the matter must be addressed or the circumstances in which LPP may be overridden. Additionally, whilst a person must have regard to a relevant code when exercising any functions to which it relates, any failure on their part to comply with the provisions of that code will not of itself make that person liable to civil or criminal proceedings.

521. Witnesses were critical of the draft Bill's approach. Peter Carter QC (who produced a recent Bar Council paper on the issue of LPP)[420] could find no protection for LPP. He did not advocate that all lawyer/client communications should be protected but referred to the Proceeds of Crime Act 2002 which, he explained, makes it clear that communications between a lawyer and a client covered by LPP are immune, but a client asking a lawyer for advice "on where the best place is to stash his stolen loot is not".[421]

417 See, for example, written evidence from BCS, The Chartered Institute for IT (IPB0075), Trading Standards North West (IPB0092), and Virgin Media (IPB0160)

418 See, for example, written evidence from the Bar Council (IPB0134), the Law Society of England and Wales (IPB0105), the Law Society of Scotland (IPB0128), the Odysseus Trust (IPB0030), Martin Chamberlain QC (IPB0133), McEvedys Solicitors & Attorneys Ltd (IPB0138), the National Union of Journalists (NUJ) (IPB0078) and the Media Lawyers Association (IPB0010)

419 Q 196 (Peter Carter)

420 Q 196 (Peter Carter)

421 *Ibid.*

EMBARGOED until 09:00 on 11 February 2016

522. Colin Passmore, who represented the Law Society, told the Committee that RIPA and the Bill were unique in conferring investigatory powers without a provision actively protecting privilege. Mr Passmore argued for the inclusion in the Bill of a specific provision reflecting the law as it stands currently across all other statutes (with the exception of RIPA) and including the iniquity provision so that if a solicitor is trying to commit a crime with their client, that information will not be protected by privilege.[422]

523. Mr Carter was concerned that the draft Bill would not allow him to reassure a client that discussions on a sensitive (but legitimate) commercial matter would definitely remain confidential. He referred to the "chilling effect" of legislation permitting access to communications, explaining that those practising in criminal law need to build up the confidence of a client so as to give robust advice.[423] If the client cannot be confident that the communication will remain confidential he or she may simply say nothing. Although not raised by Mr Carter, the same point might be made in the case of civil lawyers and their clients.

524. Mr Passmore[424] and the Law Society of Scotland[425] also raised the potential "chilling effect" when referring to the House of Lords' decision in the *McE* case.[426] Their concerns, shared by Mr Carter,[427] arose due to the Lords' finding that section 27 of RIPA (which uses the same phrase as in clauses 5 and 65 of the draft Bill, "lawful for all purposes") had the ability to enable the security and intelligence agencies, the police and others to listen in to privileged communications in those circumstances to which the case applied. Mr Passmore told the Committee that the House of Lords had been reluctant to interpret section 27 as it did because its application in this way on a regular basis would create a chilling effect on privilege, inhibiting the frankness of clients to communicate with their lawyers and potentially undermining the right to a fair trial under Article 6 ECHR, infringing privacy rights under Article 8 ECHR, and the administration of justice.[428]

525. Mr Passmore, Mr Carter, the Bingham Centre for the Rule of Law and Amnesty International UK[429] all raised similar concerns about the inclusion of LPP provisions in a code of practice. Mr Passmore considered this to be the "worst option" for dealing with the treatment of LPP, particularly as the codes do not yet exist.[430] The Committee was not able to review any codes, although we received assurances from the Home Office that they would reflect existing codes. Mr Passmore also raised the potential weakness of sanctions for a breach of a code not being based on a primary legislative provision, as in the case of both the draft Bill and RIPA.[431] By contrast, the codes of practice for the Police and Criminal Evidence Act and the Criminal Justice Act are both underpinned by a primary legislative provision.[432]

526. The issue of a code was also raised by Mr Carter who pointed out that under Schedule 6 the code would be confined to the powers exercised under part 3 (communications

422 Q 139 (Colin Passmore)
423 Q 196 (Peter Carter QC)
424 Q 137 (Colin Passmore)
425 Q 137 (Tim Musson)
426 House of Lords, *In re McE, M, C and another, [2009] UKHL 15*
427 Q 196 (Peter Carter QC)
428 Q 137 (Colin Passmore)
429 Written evidence from the Bingham Centre for the Rule of Law (IPB0055) and Amnesty International UK (IPB0074)
430 Q 141 (Colin Passmore)
431 *Ibid.*
432 *Ibid.*

EMBARGOED until 09:30 on 11 February 2016

data) and not under any other part of the Bill.[433] The Bingham Centre for the Rule of Law suggested that LPP and journalistic privilege should be addressed at the stage that a warrant is considered by a judicial commissioner, suggesting an *inter partes* hearing if viable or otherwise a hearing with special advocates.[434] As well as supporting calls for the provisions on LPP and other privileged materials to be included on the face of the Bill, Amnesty International UK also pressed for protection of the communications of NGOs like itself dealing when with sensitive cases involving human rights abuses.[435]

527. Mr Passmore told the Committee that it was the Law Society's view that, unless the Bill was amended so as to deal with privilege on its face, the concept would begin to become seriously undermined. He went on to point out that LPP rights are "current and … important" and that they are "important for the confidence of citizens in the administration of justice"..[436]

528. Mr Carter told the Committee that if LPP is not recognised as a privilege that needs to be protected, "it strikes at the heart of our judicial system."[437] JUSTICE raised similar concerns, including the lack of a specific provision addressing LPP on the face of the draft Bill, the lack of draft codes of practice to review and their limited application to communications data only.[438]

529. The Home Office's view on the Bill's treatment of LPP was put forward by Paul Lincoln, who referred to possible attempts by people to abuse the privileges available to them and explained that there was, therefore not a complete bar on such activity in terms of interception.[439] The Home Office clarified this statement, explaining that the policy intent is to make clear that special considerations apply to legally privileged material and to recognise the importance of LPP with additional safeguards set out in codes of practice. It is in the nature of the intercepting agencies' work that they will sometimes legitimately need to intercept communications between people and their lawyers in the interests of preventing or investigating serious crime or terrorist activity.[440]

530. The Home Office further explained that the draft Bill and the accompanying Codes of Practice will build on provisions in current legislation to balance the privacy of clients and patients of lawyers and doctors with the ability of law enforcement and the security and intelligence agencies to investigate wrongdoers in a manner which is not unduly fettered.[441] It acknowledged that the privilege attached to the contents of communications between lawyer and client is important and must be protected but stated also that in the course of investigations into serious criminals and terrorists, law enforcement and the security and intelligence agencies will sometimes need to intercept communications between suspects and their lawyers.[442]

EMBARGOED until 09:30 on 11 February 2016

433 Q 196 (Peter Carter)
434 Written evidence from the Bingham Centre for the Rule of Law (IPB0055)
435 Written evidence from Amnesty International UK (IPB0074)
436 Q 139 (Colin Passmore)
437 Q 196 (Peter Carter)
438 Written evidence from JUSTICE (IPB0148)
439 Q 15 (Paul Lincoln) (as clarified by the Home Office)
440 *Ibid.*
441 Written evidence from the Home Office (IPB0146)
442 *Ibid.*

531. The additional safeguards that apply to legally privileged communications are to be set out in draft codes of practice building on existing safeguards.[443] They include:

- a presumption of LPP unless the contrary is established;
- where acquiring communications subject to LPP is likely, this should be made clear in the warrant application and reasonable steps taken to minimise access to the communications subject to LPP;[444]
- where the intention is to acquire legally privileged communications, there must be exceptional and compelling circumstances which make this necessary;
- before selecting for examination material intercepted under a bulk interception warrant which is likely to include legally privileged material, an enhanced internal authorisation procedure must be followed.[445]

532. A lawyer may only be the subject of an interception/equipment interference operation in exceptional and compelling circumstances and the Home Office evidence refers to various safeguards which will be included in the code of practice. For example, material identified as legally privileged should be marked as such and only retained if necessary and proportionate and must be safeguarded from becoming available to any person whose possession of it might prejudice any criminal or civil proceedings. The acquisition and retention of legally privileged material must be reported to the relevant Commissioner. The Interception of Communications Code of Practice made under RIPA (the substance of which will, the Home Office told the Committee, be replicated under the new legislation[446]) states that a lawyer will only be targeted in exceptional and compelling circumstances.

533. The importance of Article 8 ECHR is explained in paragraph 22 of this report. Article 8 applies in the case of communications which attract LPP and it is clear that the ECtHR views such communications as deserving of particular protection. It has held that special procedural safeguards should apply in the case of a search warrant executed at a lawyer's office.[447] The precise scope of additional protections which should apply in the case of interception of documents has not been fully argued before the European Court of Human Rights but in *Kopp v Switzerland* the Court held that tapping a lawyer's telephone as part of a wider investigation into corruption was not in accordance with the law because no distinction was made between communications which would attract privilege and those which would not.[448] On the other hand a system of tapping which did provide protections to preserve the confidentiality of lawyer/client communications attracted the Court's approval.[449] This raises the question of whether the provisions in the draft Bill provide a

443 *Ibid.*

444 The reference here to a "warrant application" seems to suggest that the Code will address more than communications data as an authorisation is required in this case rather than a warrant. The same point arises in relation to the references to bulk interception warrants and equipment interference warrants. The wording used by the Home Office suggests protection for more than communications data.

445 The following Codes of Practice made under RIPA exist: Interception of Communications Code of Practice 1916, Equipment Interference Code of Practice 2016, Codes of Practice for the Acquisition, Disclosure and Retention of Communications Data 2015, Covert Surveillance and Covert Human Intelligence Sources Code of Practice 2014, Code of Practice for the Investigation of Protected Electronic Information 2010.

446 Written evidence from the Home Office (IPB0146)

447 European Court of Human Rights, *Niemietz v Germany,* (1993) 16 EHRR 97

448 European Court of Human Rights, *Kopp v Switzerland,* (1999) 27 EHRR 91

449 European Court of Human Rights, *Kruslin v France,* (1990) 12 EHRR 547 and *Huvig v France,* (1990) 1 EHRR 528

EMBARGOED until 09.30 on 11 February 2016

sufficient level of protection for LPP in so far as the ECtHR views Article 8's requirements or whether an amendment providing additional protection is necessary.

534. **The Committee is concerned that the Bill as drafted only provides (through a proposed code of practice relating to Part 3 of the Bill) for the application of LPP in the case of communications data (despite the information provided by the Home Office which suggests provisions of the code will relate to acquisition of other material).**

535. **The Committee is further concerned that there are no substantive provisions addressing LPP even in the case of communications data on the face of the Bill and considers that this may call into question the application of LPP when the Bill's powers are exercised, particularly given the judgment in *McE* and the inclusion of specific provisions in other legislation conferring investigatory powers. Additionally, the lack of a draft code prevents the Committee scrutinising provisions on an important matter.**

536. **The Committee notes the Home Office's concerns about potential abuse of privileges by either lawyers or their clients.**

537. ***The Committee recommends that provision for the protection of Legal Professional Privilege (LPP) in relation to all categories of acquisition and interference addressed in the Bill should be included on the face of the Bill and not solely in a code of practice. The Government should consult with the Law Societies and others as regards how best this can be achieved. (Recommendation 46)***

538. ***The Home Office should review its proposals in relation to LPP to ensure that they meet the requirements of Article 8 and relevant case law. (Recommendation 47)***

Journalistic Privilege

539. A number of witnesses raised concerns about the level of protection which the Bill provides for journalistic privilege. In particular, it was pointed out that the Bill dilutes the protections presently provided by the Police and Criminal Evidence Act 1984 (PACE) and the Terrorism Act 2000. Again, as with LPP, the majority of provisions relating to journalistic privilege will be included in a code of practice and relate solely to communications data. There is one provision, Clause 61 (which again relates solely to communications data), on the face of the Bill which provides that an authorisation for a relevant public authority to identify and confirm the source of journalistic information is not to take effect until approved by a judicial commissioner. This does not apply in the case of the security and intelligence agencies who do not need this approval.

540. The Media Lawyers Association (MLA) explained the present protections available to journalists and their material included in PACE and the Terrorism Act 2000.[450] Under PACE where access is required to "journalist material" (material acquired or created for the purposes of journalism) the media source involved (i.e. newspaper etc.) must be provided with certain information, in particular what material is sought, why it is believed to be of substantial value, what other methods of obtaining it have been tried and why it is believed to be in the public interest that the material should be produced or access to it provided. There is also "excluded material" which is very infrequently accessed using PACE but can

450 Written evidence from the Media Lawyers Association (IPB0010)

EMBARGOED until 03:30 on 11 February 2016

be obtained under the Terrorism Act 2000 provided that the material is sought for the purposes of a terrorism investigation and the officer has reasonable grounds to believe the material will be of substantial value and should be produced. In the case of both journalistic and excluded material there must be an overriding public interest requiring disclosure and applications must normally be heard by a judge on notice, providing the judge with evidence and argument from both parties and ensuring that the journalist has an opportunity to make a case against disclosure if they feel this is appropriate.

541. Journalists have found themselves without these safeguards in a number of instances where the Police have sought to make use of RIPA provisions which do not require judicial approval for the interception, acquisition and disclosure of communications data and covert and human surveillance. As well as side-stepping the need for judicial approval a number of Police forces also failed to comply with relevant requirements (now contained in the RIPA Acquisition and Disclosure of Communications Data Code of Practice 2015) relating to the authorisation of police activity under RIPA.[451]

542. The MLA raised Articles 10 and 6 of the European Convention on Human Rights.[452] Article 10(1) provides that everyone has the right to freedom of expression which includes freedom to receive and impart information and ideas without interference by public authority. The right is a qualified one: it may be subject to such:

> "formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary".

The MLA suggested that an order requiring the handing over of journalistic material both engages Article 10 ECHR and amounts to an interference under Article 10(1). It will only be justified if it is prescribed by law, proportionate and necessary in view of one of the matters listed in Article 10. Additionally, the MLA suggested that the right to a fair hearing under Article 6 is also engaged and emphasised the importance of *inter partes* hearings enabling the media to make informed representations before material is accessed or obtained. Whilst such hearings are held under PACE and the Terrorism Act, they are not provided for under either RIPA or under the draft Bill which provide for *ex parte* applications. This raises the question of compatibility of provisions of the draft Bill with ECHR Articles. Provisions which guaranteed *inter partes* hearings would help to minimise the risk of arrangements falling foul of Article 6.

543. The MLA acknowledged that the draft Bill gives explicit protection to journalists but was concerned that at the same time it creates a route whereby the state can identify a source without going through PACE protections.[453] Further, it expressed concern that Clause 61 deals solely with communications data and there are no specific protections in relation to any other powers of collection and retention. Additionally, it noted, whilst Clause 61 requires that an application relating to communications data be approved by a judicial commissioner, the procedure is linked to proposed codes and not to provisions

451 Written evidence from the Media Lawyers Association (IPB0010) and JUSTICE (IPB0148)
452 Written evidence from the Media Lawyers Association (IPB0010)
453 *Ibid.*

EMBARGOED until 09:30 on 11 February 2016

on the face of the draft Bill. Further, the MLA noted that applications to a judicial commissioner can be made without prior notification to the media organisation involved which would also have no right to contest an application before a judicial commissioner. Additionally, it noted that the draft Bill does not provide a right to source protection and further the ability to obtain data is not limited to specific activities. Finally, it told the Committee it will be possible for those seeking information to evade PACE by using the powers provided by the draft Bill.[454]

544. The MLA's concerns were shared by a number of witnesses.[455] Andy Smith, representing the National Union of Journalists (NUJ), referred to the system of prior notification which exists under PACE and which offers the opportunity to explain a situation, so that a judge can make a variation of an application made to him (which may lead to the disclosure of less material than is sought), which, the NUJ considered would very difficult under the proposed framework.[456] He also said that PACE means that journalists are supplied with sufficient information about an application, for instance what other means have been attempted to obtain the information and a face-to-face hearing enables journalists to demonstrate, particularly to potential sources of information, their commitment to source protection. The draft legislation would not afford a right to appeal for a journalist.

545. In its written submission the NUJ echoed the views set out in its oral evidence, in particular in respect of prior notification of applications for journalistic material.[457] Further, it noted that there is no prior right of notification for journalists or media organisations where their material is either deliberately, incidentally, collaterally or accidentally sought or obtained, whether by the police or by intelligence agencies and the proposed measures can be bypassed by using urgency procedures.

546. The NUJ was also concerned (as was the MLA and JUSTICE[458]) that the police will now start using the draft Bill's powers routinely to identify sources instead of making PACE/Terrorism Act applications for a journalist's material as they consider that the draft Bill provides an easier route for the authorities to identify a journalists' source when it is compared to PACE. It agreed with other witnesses that the production order procedures set out in PACE offer better safeguards and protections than those proposed in the draft Bill. It also argued that the draft Bill's current proposals would not allow journalists to protect the identity of sources or provide sufficient protections for journalists' materials and communications (a right recognised by the ECtHR) as laid down in its Code of Conduct.[459] This could result in informers being unwilling to speak out and also in journalists being perceived as informers possibly impacting on their safety in certain instances. It also noted that the proposed oversight will only apply for the purpose of an application to identify a journalistic source and the judicial authorisation set out in the draft Bill will only cover the police and not the security and intelligence agencies.[460] The Union was also concerned by the broad nature of powers on "equipment interference" and the access which they will provide for authorities. The NUJ concluded that the draft Bill needs better safeguards and not just in the section relating to the interception of communications data.[461]

454 *Ibid.*
455 See, for example, Q 140, 142 (Bob Satchwell, Society of Editors)
456 Q 142 (Andy Smith, National Union of Journalists)
457 Written evidence from the National Union of Journalists (IPB0078)
458 Written evidence from the Media Lawyers Association (IPB0010) and JUSTICE (IPB0148)
459 Q 144 (Andy Smith, National Union of Journalists)
460 Written evidence from the National Union of Journalists (NUJ) (IPB0078)
461 *Ibid.*

EMBARGOED until 09:30 on 11 February 2016

547. Guardian News and Media referred to the public interest role of newspapers in ensuring continual oversight and accountability of public and private institutions.[462] It shared concerns that the draft Bill creates a route by which information can be accessed without compliance with the safeguards as set out in PACE. It argued that the Bill does go far enough in giving explicit protection to journalists and that Clause 61 and the requirement that statutory Codes of Practice be issued in respect of communications data must make provision for additional safeguards for sensitive professions. It also expressed concern as to the assessment which would be made by a judicial commissioner stating that it would be no more than a "review of a police decision, already taken, against an extremely broad standard".[463]

548. The News Media Association (NMA) also felt that the draft Bill would not ensure adequate protection for freedom of expression as it does not provide sufficient substantive or procedural protections for press freedom.[464] The draft Bill would, in its view, "enshrine sweeping powers affecting journalists and their sources, leaving unchanged other RIPA surveillance powers used against the press". It would, it considered, allow the relevant authorities to evade satisfaction of the stringent tests necessary for proper safeguard of press freedom and would also continue to permit the police to bypass the statutory protections laid down in PACE and the Terrorism Act 2000.[465] The draft Bill should, it suggested, contain provisions akin to PACE, allowing prior notification and challenge of applications as well as stronger conditions for grant of an application and a right of speedy media appeal.

549. In NMA's view there is a need for "comprehensive and stronger safeguards than those found in draft Bill" as otherwise the relevant authorities would still be able to make unwarranted use of the powers relating to intrusive and covert surveillance under RIPA 2000 and all the powers governed by the draft Bill including interception of communications; obtaining of communications data and of equipment interference.[466] It explained that these powers could be used for tracking individual journalists, investigative teams, the entire editorial staff of media organisations and the subject, progress, course and content of their investigations including outside sources and confidential sources. The provisions permit access, accumulation and sifting of journalistic information gathered, with the risk of its use or disclosure for other purposes.

550. In the case of the proposed codes relating to the exercise of the other powers under the Bill against journalists, NMA made the point that RIPA surveillance codes have proved inadequate protection to date. It went on to suggest that the role of the Judicial Commissioner does not allay media concerns in view of the judicial review test which a Commissioner is to apply (see paras 422–433). NMA's view was that this does not enable a rigorous test of an application's merit. The Minister and the Judicial Commissioner's evaluations will not benefit from hearing media challenge and contradiction of the applicants' assertions and/or of Ministerial acquiescence. Further, NMA noted that the judicial commissioner is only to apply the principles of judicial review to the Ministerial consent. This, it was suggested, does not enable "rigorous test of the applications' merit".[467]

462 Written evidence from Guardian News & Media (IPB0040)
463 *Ibid.*
464 Written evidence from News Media Association (IPB0012)
465 *Ibid.*
466 *Ibid.*
467 *Ibid.*

EMBARGOED until 09.30 on 11 February 2016

551. NMA's view was representative of that of other journalistic witnesses: "Clause 61 must be improved, but this must be in conjunction with the addition of other clauses introducing the PACE type press freedom protections and procedures necessary in relation to all applications and use of powers under the RIPA and IP legislation".[468] In the case of the proposed codes relating to the exercise of the other powers under the Bill against journalists NMA made the point that RIPA surveillance codes have proved inadequate protection to date. The Minister and the Judicial Commissioner's evaluations will not benefit from hearing media challenge and contradiction of the applicants' assertions and/or of Ministerial acquiescence.

552. Issues were raised over the definition of journalists. This was highlighted by Andy Smith from the NUJ who said "I have seen various definitions. The advantage of PACE is that it does not define a journalist, and in some ways that is safer… Frankly, some very good journalistic work is being done on the internet by people who are not associated with the traditional media outlets. There is a debate to be had there, but I would say it is developing."[469]

553. **The Committee considers that protection for journalistic privilege should be fully addressed by way of substantive provisions on the face of the Bill.**

554. ***The Committee recommends that the Home Office should reconsider the level of protection which the Bill affords to journalistic material and sources. This should be at least equivalent to the protection presently applicable under PACE and the Terrorism Act 2000. (Recommendation 48)***

555. ***The Committee recommends that if Clause 61 remains in its present form the Bill should make it clear that RIPA and Clause 61 do not act so as to enable the investigatory authorities to avoid the application of PACE or the Terrorism Act and the ability they afford to media to know about an application for communications data and make representations as to the proposed acquisition. (Recommendation 49)***

556. ***The Home Office should review Clause 61 to ensure that it meets the requirements of Article 10 ECHR. (Recommendation 50)***

Parliamentary Privilege

557. The Bill contains a specific provision addressing an application for a targeted interception or examination warrant in the case of a person who is a member of a relevant legislature (which includes members of the Houses of Parliament, as well as members of the devolved Parliaments and Assemblies and the European Parliament). Before the Secretary of State authorises such a warrant she or he must consult the Prime Minister.

558. Additionally, Schedule 6 of the draft Bill provides for a code of practice about the exercise of functions under Part 3 of the draft Bill (i.e. in relation to communications data). The code must include provision about particular considerations applicable to any data which relates to, *inter alia*, MPs on the basis that they enter into communications with their constituents. The precise meaning of this provision is not clear partly as the relevant code does not presently exist but it will only apply to communications data related to communications between MPs and their constituents.

468 *Ibid.*
469 Q 143 (Andy Smith, National Union of Journalists)

EMBARGOED until 09:30 on 11 February 2016

559. The draft Bill does not enshrine in law what is known as the "Wilson doctrine" which provides for the interception of the communications of MPs and further provides that any change in the policy of interception will be made known to MPs at such moment as seems compatible with the security of the country.

560. David Davis MP suggested that he would remove the role of the Prime Minister in the interception of politicians' communications as he was uneasy about a politician deciding on whether or not to tap a politician's phone.[470] Additionally the draft Bill refers to MPs and their constituents which he considered to be probably the least interesting to the agencies of an MP's communications. He suggested that communications with whistleblowers and journalists would be likely to be of more interest. Further, he noted that communications data is not subject to the Wilson Doctrine even though it has become more significant in recent years.[471]

561. Dr Andrew Defty of Lincoln University suggested that legislation relating to the interception of communications passed since the 1980s means that the Wilson Doctrine is now out of step with the current statutory framework and that the draft Bill provides an opportunity to place the Doctrine on a statutory footing, if the intention is that the communications of parliamentarians should be treated differently to those of other members of the public.[472] He suggested that this could have been achieved by a process where the Prime Minister informed the ISC (or its chair) if a warrant were issued to intercept the communications of a member of a relevant legislature. He noted the draft Bill's extension of protections to members of other legislatures.[473]

562. Professor Christopher Forsyth, when asked about the safeguard of Prime Ministerial approval under Clause 16, suggested that whilst it was understandable that individual MPs of one party might not believe that the Prime Minister is much of a safeguard when he belongs to a directly opposed party, the judicial commissioner is there to see that there is no skulduggery in the approval of the warrant and if the judicial commissioner refuses, it is not going to get to the Prime Minister.[474] He went on to add that the precise mechanics of how Clause 16 would work are not clear. It may be that review by a judicial commissioner is necessary before the Prime Minister's approval is sought but the sequence of events is not spelt out in the Clause.

563. The Home Secretary was asked why the Wilson Doctrine is not enshrined in the Bill and why the Bill does not require the Prime Minister to make a declaration to Parliament.[475] She explained that the IPT had recently found that the Wilson Doctrine was still in place and that the definition of it was as she had set out to the House of Commons.[476] She went on to add that the most important element of the Doctrine is included in the Bill. This is the a requirement, where it is suggested that there be interception in relation to, not just a Member of Parliament but Members of the House of Lords, UK MEPs and Members of the devolved assemblies and parliaments, for the Prime Minister to be consulted on the use of the interception power. Further, she suggested that the Prime Minister had made it clear that the aspect of the Wilson Doctrine dealing with the Prime Minister making

470 Q 185 (David Davis MP)
471 *Ibid.*
472 Written evidence from Dr Andrew Defty (IPB0050)
473 *Ibid.*
474 Q 221 (Professor Christopher Forsyth)
475 Q 280 (Theresa May MP)
476 HC Deb, 19 October 2015, col 700

EMBARGOED until 09:30 on 11 February 2016

a statement to the House when policy changed in relation to the Doctrine still applied. But she did not think it appropriate to put that element of the Doctrine on the face of a piece of primary legislation. The Home Secretary suggested that there may be some misunderstanding about the statement to Parliament that the Prime Minister makes. She explained that the statement would be about any change of policy governing the interception of MPs, not that there has been an instance of such interception. Generally, she explained, statements about changes of policy on a whole range of matters are regularly made to Parliament. No requirement for the Government to do make these statements is on the face of any legislation.[477]

564. **The Committee considers that the approach taken in the Bill to surveillance of Parliamentarians strikes an effective balance between the need for Parliamentarians to be able to communicate fully and frankly with their constituents and other relevant third parties and the needs of the security and intelligence agencies and law enforcement agencies.**

EMBARGOED until 09:30 on 11 February 2016

477 Q 280 (Theresa May MP)

5 Oversight

565. The approach to oversight in any investigatory powers regime is crucial to the compliance of that regime with the protection of individual rights under the European Convention on Human Rights and European Union law. As noted above at paragraphs 17–24, the law in this area remains under development and there is no legal checklist that can be applied to the proposed regime to ensure it remains compliant with the Government's obligations to protect individual rights. Martin Chamberlain QC told us:

> "The question whether existing oversight mechanisms satisfy Article 8 standards is itself currently before the European Court of Human Rights. The outcome of that litigation may not be known before this Bill is enacted. It is likely to be highly material to the question whether the safeguards in the Bill are compliant with Article 8."[478]

566. Under the present state of the law legally compliant oversight requires a role for a body that is not only independent of the executive in reality but is seen to be independent of the state.[479] Public perception of the relationship between the executive and the oversight body is also relevant. Martin Chamberlain QC told us that "Parliament's aim at this stage should be to make the statutory safeguards as robust as possible so as to give the Bill the best chance of being held compatible with Article 8."[480]

Current oversight regime

567. Three Commissioners, appointed under RIPA, have general scrutiny functions. Each of the Commissioners is a retired High Court or Court of Appeal judge. Each is appointed by the Prime Minister and reports to him. Oversight of the intelligence agencies, save for their interception practices, is carried out by the Intelligence Services Commissioner, currently Sir Mark Waller. The Interception of Communications Commissioner, currently Sir Stanley Burnton, oversees the interception of communications by the intelligence and law enforcement agencies which are permitted by Chapters 1 (interception) and 2 (acquisition and disclosure of communications data) of Part 1 of RIPA. The Chief Surveillance Commissioner, currently Lord Judge, oversees public authorities' use of their RIPA powers for covert surveillance in public and private places, the use of covert human intelligence sources and property interference.

568. David Anderson QC reported that the system of Commissioners "came in for considerable criticism from civil society" including that the range of Commissioners and division between their responsibilities created confusion and meant that no one Commissioner was sufficiently well-placed to assess the proportionality of measures taken; that they were insufficiently public facing; that they were insufficiently independent of Government; that as judges they were ill-suited to inquisitorial work; and that their work was insufficiently probing.[481] There were also concerns over the adequacy of the resources available to support the Commissioners in their work. RUSI agreed that the commissioners were part of an oversight regime which was overly complex and poorly understood and

478 Written evidence from Martin Chamberlain QC (IPB0133)

479 European Court of Human Rights *Klass v Germany* (1978) 2 EHRR 214 and *Zakharov v Russia* (2015) application no. 47143/06

480 Written evidence from Martin Chamberlain QC (IPB0133)

481 David Anderson QC, *A Question of Trust: Report of the Investigatory Powers Review*, 2015, para 12.86

EMBARGOED until 09.30 on 11 February 2016

that "Reorganisation and better resourcing of the existing setup could create a more streamlined, robust and systematic oversight regime that would be genuinely visible to the public and have a positive effect on the police and SIAs."[482] The ISC recommended "an increased role for the Commissioners" and for their non-statutory functions to be given a statutory footing. ISC also suggested that there could be a case for pooling resources between the three Commissioners.[483]

569. The Anderson report recommended that the three current Commissioners should be replaced by an Independent Surveillance and Intelligence Commission (ISIC). ISIC would fulfil the intelligence oversight function currently carried out by the Intelligence Services Commissioner, together with the auditing functions of the three. It would retain the Chief Surveillance Commissioner's role in relation to approvals and issuing guidance. In addition ISIC would also have oversight of the acquisition and use of communications data, the use of open-source intelligence and the sharing and transfer of intercepted material and data. As discussed above, ISIC would take over the judicial authorisation of all interception warrants and some categories of requests for communications data.[484]

Commissioners or a Commission?

570. Clause 167(6) of the draft Bill provides that the "Investigatory Powers Commissioner and the other Judicial Commissioners are to be known, collectively, as the Judicial Commissioners." The Interception of Communications Commissioner's Office (IOCCO) raised concerns with us that this approach failed to acknowledge "the reality" that the Judicial Commissioners themselves would "only be performing a very narrow part of the oversight—the prior authorisation of some of the more intrusive investigatory powers. The bulk of the oversight will actually be carried out by inspectors and staff within the Commission."[485] To ensure "effective" oversight the IOCCO said the inspectors need a "clear legal mandate to require information from public authorities, to launch and undertake audits, inspections, inquiries, investigations and react in real time when non-compliance or contraventions of the legislation are discovered during an inspection."[486]

571. The duty imposed on the Investigatory Powers Commissioner in Clause 169(1) to "keep under review (including by way of audit, inspection and investigation) the exercise by public authorities of" the relevant powers. IOCCO said that this position did not "compare favourably with the clear powers and legal mandate in place for some of our international counterparts."[487] JUSTICE agreed that the draft Bill failed to make it clear that the Investigatory Powers Commissioner had the power to conduct inquiries "on its own initiative about the operation of the legal framework within its sphere of responsibility."[488] The IOCCO concluded that a Commission created as a body corporate with statutory powers vested in both the institution and the Judicial Commissioners would meet its

EMBARGOED until 09:30 on 11 February 2016

482 Royal United Services Institute (RUSI), *A Democratic Licence to Operate: Report of the Independent Surveillance Review*, July 2015, p.xii

483 Intelligence and Security Committee (ISC), *Privacy and Security: A modern and transparent legal framework*, 12 March 2015, HC 1075, Recommendation JJ

484 David Anderson QC, *A Question of Trust: Report of the Investigatory Powers Review*, 2015

485 Written evidence from the Interception of Communications Commissioner's Office (IPB0101)

486 *Ibid.*

487 *Ibid.*

488 Written evidence from JUSTICE (IPB0148)

concerns. The IOCCO told us that a precedent for this model of oversight could be found in the Independent Police Complaints Commission.[489]

572. The Anderson report recommended the creation of a single oversight body for all surveillance powers, an "Independent Surveillance and Intelligence Commission (ISIC)."[490] In his written evidence to us, Mr Anderson said the creation of a Commission was necessary if the oversight body established by the draft Bill was to "fulfil its potential as a well-informed, independent and authoritative guarantee that some extraordinarily extensive powers are not misused."[491]

573. The Home Office did not comment specifically on why it had chosen the Judicial Commissioners model rather than creating a Commission. In written evidence it referred to the benefit of having one senior independent judicial figure in the Investigatory Powers Commissioner who, by having ultimate responsibility, "will help ensure consistent standards between the users of investigatory powers and allow best practise to be shared."[492]

574. **It is unclear to us why the Home Office chose to create a group of Judicial Commissioners rather than creating an Independent Intelligence and Surveillance Commission as recommended by David Anderson QC, a recommendation endorsed by the knowledgeable and experienced Interception of Communications Commissioner's Office. The benefits of having a senior independent judicial figure in the Investigatory Powers Commissioner would not be lost by putting the IPC at the head of a Commission. The evidence we have heard is that the work of the oversight body will be significantly enhanced by the creation of a Commission with a clear legal mandate.** ***We recommend that such a Commission should become the oversight body in the Bill. (Recommendation 51)***

575. ***The Judicial Commissioners or Commission should have the power to instigate investigations on their or its own initiative. This is vital in order to ensure effective and independent oversight. The current provisions in the draft Bill on the powers of the Judicial Commissioners do not make it clear that they have this power. We recommend that a power to initiate investigations should appear on the face of the Bill. (Recommendation 52)***

Judicial Commissioners

576. The draft Bill provides for the appointment for an unspecified number of Judicial Commissioners under the authority of an Investigatory Powers Commissioner. The role of the Judicial Commissioner in authorising warrants has been referred to as introducing "judicial authorisation" into the regulation of investigatory powers. The proposed structure for appointing, re-appointing, dismissing and funding Judicial Commissioners differs in a number of respects from that of senior judges in the ordinary courts.

EMBARGOED until 09:30 on 11 February 2016

489 Written evidence from the Interception of Communications Commissioner's Office (IPB0101)
490 David Anderson QC, *A Question of Trust: Report of the Investigatory Powers Review*, 2015, Recommendation 82
491 Written evidence from David Anderson QC (IPB0152)
492 Written evidence from the Home Office (IPB0146)

Creation of a single oversight body

577. Witnesses welcomed the creation of a single body to oversee the use of powers under the Bill. Lord Judge, the Chief Surveillance Commissioner, told us:

> "I cannot think that anyone would have designed the present three-bodied system. It would never have happened; it should not have done. We work piecemeal on the legislation; we produce piecemeal results; and we have produced three bodies, all of which have responsibilities in the broad sense that we are talking about and all of which work in different ways."[493]

578. McEvedys Solicitors agreed with Lord Judge that system of three commissioners "was confusing to the public, and created the potential for duplication. More importantly, it reduced transparency and undermined the ability of any of them to build public confidence in the investigatory powers."[494] The only concern we heard over the replacement of the three commissioners by one was from Sir Mark Waller who expressed concern that the resulting workload may be too much for one Commissioner.[495] This concern should be addressed by the fact a number of Commissioners will be appointed and the Investigatory Powers Commissioner has an explicit power to delegate his functions when required (Clause 167(7)).

579. **We welcome the creation of the Judicial Commissioners as a single oversight body which will improve transparency, public confidence and effective oversight of the use of the powers contained in the Bill.**

Appointment

580. The draft Bill requires that the Prime Minister appoint an Investigatory Powers Commissioner and "such number of other Judicial Commissioners as the Prime Minister considers necessary for the carrying out of the functions of the Judicial Commissioners."[496] Judicial Commissioners must hold or have previously held office as a senior judge.[497]

581. Witnesses raised concerns over the impact of appointment by the Prime Minister on the perceived independence of Judicial Commissioners and the consequent impact on public confidence in the oversight regime. The Interception of Communications Commissioner's Office (IOCCO) told us: "It is inappropriate for the Judicial Commissioners to be appointed by the Prime Minister as this dilutes public confidence and independence."[498] Sir Mark Waller, the Intelligence Service Commissioner, agreed that the "public perception" of the Judicial Commissioners' independence could be affected by prime ministerial appointment.[499] We heard from the United Nations Special Rapporteurs, that the Prime Ministerial power to appoint "compromises the independence and impartiality of the Judicial Commissioners".[500] Liberty said that the impact on public perception of appointment by the Prime meant the oversight structure proposed by the

493 Q 47 (Lord Judge)
494 Written evidence from McEvedys Solicitors (IPB0138) See also written evidence from Liberty (IPB0143)
495 Q 40 (Sir Mark Waller)
496 Clause 167(1)
497 Clause 167(2). Senior judge is used as defined in Part 3 of the Constitutional Reform Act 2005.
498 Written evidence from the Interception of Communications Commissioner's Office (IPB0101)
499 Q 46 (Sir Mark Waller)
500 Written evidence from the UN Special Rapporteurs (IPB0102)

EMBARGOED until 09:30 on 11 February 2016

draft Bill could not amount to "world leading oversight".[501] Lord Carlile of Berriew CBE QC told us: "It is … of high importance that the Judicial Commission does not become politicised. This is a possibility if one body oversees all investigatory powers. Selection of the Judicial Commissioners should remain independent of Government, and placed in the hands of the Lord Chief Justice for the time being."[502] These views were expressed in similar terms by several other witnesses.[503]

582. Some support for appointment by the Prime Minister came from Professor Clarke, Retiring Director of the Royal United Services Institute, who told us that the Judicial Commissioners would have to "enjoy the confidence of the Prime Minister and the political establishment" as well as inspiring public confidence.[504]

583. Proposed alternatives to appointment by the Prime Minister focused on roles for the Judicial Appointments Commission and Lord Chief Justice or a hybrid of the two. Drs Cian Murphy and Natasha Simonsen, Law Lecturers at King's College, London, recommended appointment by the Judicial Appointments Commission, on the grounds that:

> "The draft Bill places upon the Judicial Commissioners an obligation to serve in what is, in effect, a quasi-judicial role. We recommend (below) that that role be made as close to a judicial role as possible—a key part of which is appointment through an appropriate process. We consider that appointment through the Judicial Appointments Commission will build public confidence, and is more likely to command the respect of overseas stakeholders, including foreign Governments and communications service providers."[505]

584. Peter Carter QC agreed that the Judicial Appointments Commission should be responsible for appointments to avoid the public perception that they were "political appointment[s]" but suggested a consultative role for the Lord Chief Justice.[506] Lord Judge, Chief Surveillance Commissioner, told us that for practical and constitutional reasons appointment should be by the Lord Chief Justice when serving judges were under consideration. He noted that deployment of judges currently in office was a "crucial responsibility" of the Lord Chief Justice "who not only has the clearest understanding of the experience and skills of all the judges, but who also knows those judges who will be serious candidates for the Court of Appeal where new experiences as commissioners would be valuable."[507] In addition the Lord Chief Justice "will have to address the consequences of the drain on judicial resources in the High Court and Court of Appeal of seconding senior judges to the Commission" a point echoed by JUSTICE which suggested that "any drain on the High Court when judges take up appointments as Judicial Commissioners should be offset by the Treasury."[508] Lord Judge concluded that "for judges currently in office the only viable system is for the Lord Chief Justice to assign them to work as

EMBARGOED until 09:30 on 11 February 2016

501 Written evidence from Liberty (IPB0143)
502 Written evidence from Lord Carlile of Berriew CBE QC (IPB0017)
503 For example, written evidence from the Bar Council (IPB0134), Privacy International (IPB0120) and Cian C Murphy and Natasha Simonsen (IPB0096)
504 Q 69 (Professor Michael Clarke)
505 Written evidence from Cian C Murphy and Natasha Simonsen (IPB0096)
506 Q 193
507 Written evidence from Lord Judge (IPB0020)
508 Written evidence from JUSTICE (IPB0148)

Commissioners."[509] The Lord Chief Justice's 2015 Annual Report noted that High Court Judges had recently experienced a significant increase in their workload.[510]

585. We also heard suggestions for adapting the proposed appointment process. David Anderson QC proposed a consultative role for the Lord Chief Justice, the involvement of the Judicial Appointments Commission and "possibly some sort of parliamentary hearing. For the purposes of public perception, that may be a good idea."[511] Lord Judge had concerns over the workload of the Judicial Appointments Commission and the length of time appointments could take. He suggested that the process undertaken for the last commissioner appointed to his team should be used: "a senior serving judge and a member of the Judicial Appointments Commission sat together, with my predecessor as an observer, and they chose whom it should be, and the appointment was then made."[512]

586. We were interested to hear from the Home Secretary, Theresa May, that appointment of a sitting judge would "be a matter more for the Lord Chief Justice and for advice from the Lord Chief Justice. Indeed, the intention is that the Lord Chief Justice would be making nominations to the Prime Minister."[513] Mrs May rejected the suggestion that appointment by the Prime Minister would have any implications for the independence of Judicial Commissioners on the grounds that the current commissioners were prime ministerial appointees and "there is no suggestion that they have not been independent in the operation of the work that they have done."[514]

587. **We do not think that appointment by the Prime Minister would in reality have any impact on the independence of the Investigatory Powers Commissioner and Judicial Commissioners. In modern times, our senior judges have had an unimpeachable record of independence from the executive and we believe any senior judge appointed to these roles would make his or her decisions unaffected by the manner of appointment.**

588. ***We recommend that the Lord Chief Justice should have the power to appoint Judicial Commissioners following consultation with his judicial counterparts in Scotland and Northern Ireland and with the Prime Minister, Scottish Ministers, and the First Minister and deputy First Minister in Northern Ireland. This will ensure public confidence in the independence and impartiality of the Judicial Commissioners. It will also enhance political confidence in them. The Lord Chief Justice will also be able to assess the impact of appointments on the work of the High Court and the Court of Appeal, which must not be impaired by the creation of the Judicial Commissioners. The Judicial Appointments Commission must also be consulted to ensure that the appointments procedure is fair and transparent. (Recommendation 53)***

Re-appointment and length of terms

589. The draft Bill states that appointments are for three years and are renewable.[515] Some criticism of these provisions was focused on the interaction between this provision and the role of the Prime Minister in appointing Judicial Commissioners. The Center for

509 Written evidence from Lord Judge (IPB0020)
510 The Lord Chief Justice, *The Lord Chief Justice's Report 2015*, January 2016
511 Q 69 (David Anderson QC)
512 Q 59 (Lord Judge)
513 Q 280 (Teresa May MP)
514 *Ibid.*
515 Clause 168(2) and (3)

EMBARGOED until 09:30 on 11 February 2016

Democracy and Technology told us that it was the combined effect of "the appointment process and potentially indefinite renewable terms" which would "prevent" the Judicial Commissioners from being "fully independent of the executive."[516] Privacy International was opposed to appointment by the Prime Minister but told us its concerns of the impact executive appointment would have on the independence of the Judicial Commissioners were "exacerbated" by the "brevity and renewable nature of these terms".[517]

590. The Bingham Centre for the Rule of Law said that terms of appointment should not be renewable because "[i]t is important that there be absolutely no possibility of perception that a Commissioner's decisions could be influenced by a desire to have a term renewed."[518] David Anderson QC, the Independent Reviewer of Terrorism Legislation, saw the "advantages of a single term" so that "there would be no question of people being careful around the renewal period." He observed that he was appointed for a three-year renewable term: "Did that affect the timing of any fights I might have wanted to pick with the Home Secretary? I do not know; perhaps subconsciously it did."[519]

591. There was no consensus on how long appointments should be. Professor Clarke was not opposed to the power to renew appointments but preferred longer terms of four or five years "so that somebody could build a greater profile in the work that they do, which the public would get used to."[520] The Bingham Centre for the Rule of Law suggested that Judicial Commissioners should be able to opt for a non-renewable term of three, four or five years if the Prime Minister continued to have the power of appointment.[521] David Anderson QC thought that serving judges may be reluctant to become Judicial Commissioners if required to do it for much longer than three years as it could pose difficulties for their return to "regular judging".[522] Peter Carter QC agreed and observed that the potentially "onerous" nature of the role could mean that three years "would probably be sufficient" for retired judges to "feel that they have done their job and would quite like to go and do something else."[523] Matthew Ryder QC suggested that the Judicial Appointments Commission be consulted on the appropriate tenure for the role as it has "done some significant thinking on how long tenures should be for judges, to ensure that judges do not feel vulnerable when they next come up for review."[524] The longest tenure suggested was a non-renewable term of seven years which is the approach taken in the United States for judges appointed to the Foreign Intelligence Surveillance Court.[525]

592. **We accept concerns that having renewable terms of appointment could have negative implications for public confidence in the independence of Judicial Commissioners. We conclude that these concerns strengthen the argument for the power of appointment being held by the Lord Chief Justice, rather than the Prime Minister.**

593. ***The Government should reconsider both the length of terms of appointment and whether they should be renewable. Terms need to be long enough for Judicial Commissioners to build expertise but should not be so long that they have a negative***

516 Written evidence from the Center for Democracy & Technology (IPB0110)
517 Written evidence from Privacy International (IPB0120)
518 Written evidence from the Bingham Centre for the Rule of Law (IPB0055)
519 Q 69 (David Anderson QC)
520 Q 69 (Professor Michael Clarke)
521 Written evidence from the Bingham Centre for the Rule of Law (IPB0055)
522 Q 69 (David Anderson QC)
523 Q 193 (Peter Carter QC)
524 Q 193 (Matthew Ryder QC)
525 Written evidence from the Center for Democracy & Technology (IPB0110)

EMBARGOED until 09:30 on 11 February 2016

impact on a serving judge's career. It may be that three-year terms with an option for renewal is the most workable solution but we recommend that there should be careful reconsideration of these provisions in consultation with the Lord Chief Justice, Judicial Appointments Commission, the current surveillance Commissioners and other interested parties to ensure the benefits and disadvantages of the different approaches have been thoroughly examined. (Recommendation 54)

Dismissal

594. Judicial Commissioners can be removed from office following a resolution in both Houses of Parliament.[526] A Judicial Commissioner can be removed from office by the Prime Minister for being sentenced to imprisonment following conviction for a criminal offence,[527] for bankruptcy,[528] disqualification as a director of a company[529] and for being the subject of specified orders under the Insolvency Act.[530] The Investigatory Powers Commissioner, in consultation with the Prime Minister, can end a Judicial Commissioner's term of appointment for "inability" or "misbehaviour"[531] or for "a ground specified in the Judicial Commissioner's terms and conditions of appointment."[532]

595. The proposed powers to remove Judicial Commissioners from office differ markedly from those applicable to senior judges. The senior judiciary can be removed from office only by a resolution of both Houses of Parliament. Section 108 of the Constitutional Reform Act 2005 provides that the Lord Chief Justice can suspend a senior judge who is "subject" to criminal proceedings; is serving a sentence imposed in criminal proceedings; or who "has been convicted of an offence and is subject to prescribed procedures in relation to the conduct constituting the offence." Senior judges may be suspended during proceedings for by Address in Parliament to remove them from office. The power to suspend a member of the senior judiciary can only be exercised by the Lord Chief Justice with the agreement of the Lord Chancellor.[533]

596. Concerns over the drafting of these clauses and their impact on the independence of the Judicial Commissioners were expressed by the Bingham Centre for the Rule of Law. The Centre noted that "inability" and "misbehaviour" were not defined in the draft Bill. The Centre also expressed concern that the provision to allow removal from office for breaching the terms and conditions of appointment was potentially disproportionate given "we doubt that all terms and conditions should carry equal weight in decisions about removal from office."[534] Specific criticism of the drafting aside, the Bingham Centre concluded that protecting the independence of the Judicial Commissioners required that "removal from office on the grounds of inability to carry out the functions of a Commissioner or misbehaviour requires a resolution of each House of Parliament, except under subsection (5)."[535] A group of non-governmental organisations operating in the United States in the field of democracy and technology also expressed concern that dismissal of Judicial

526 Clause 168(4)
527 Whether the sentence of imprisonment is suspended or not Clause 168(5)(d)
528 Clause 168(5)(a)
529 Clause 168(5)(b)(i) and 168(5)(c)
530 Clause 168(5)(b)(ii) and (iii)
531 Clauses 168(6)(a) and 168(7)
532 Clauses 168(6)(b) and 168(7)
533 Constitutional Reform Act 2005, section 180
534 Written evidence from the Bingham Centre for the Rule of Law (IPB0055)
535 *Ibid.*

EMBARGOED until 09:30 on 11 February 2016

Commissioners was possible "on grounds not set out in the legislation."[536] The Interception of Communications Commissioner's Office did not criticise the provisions themselves but recommended that the Lord Chief Justice be consulted before the power to dismiss was exercised.[537]

597. ***Maintaining public confidence in the Judicial Commissioners may occasionally require that a Commissioner is removed from the role because he or she has behaved in a manner incompatible with what is, in effect, high judicial office. Public confidence also requires that the power to remove from office does not damage the public perception of the Judicial Commissioners' independence from the executive or the freedom of the Judicial Commissioners to make decisions that may be unpopular with the Government. We believe that the broad powers of dismissal contained in the draft Bill significantly impair the independence of the Judicial Commissioners. We therefore recommend that the Judicial Commissioners be subject to the same dismissal and suspension procedures as those applicable to serving senior judges: removal from office following a resolution of both Houses of Parliament and suspension and other disciplinary measures exercised by the Lord Chief Justice and Lord Chancellor. (Recommendation 55)***

Funding

598. Clause 176(1) of the draft Bill provides that Judicial Commissioners will be paid "out of money provided by Parliament such remuneration and allowances as the Treasury may determine." Funding other than the pay of the Judicial Commissioners themselves is a matter for the Home Secretary in consultation with the Investigatory Powers Commissioner and subject to the approval of the Treasury.[538] The Explanatory Notes state that: "Should the Investigatory Powers Commissioner believe that the resources afforded to them are insufficient then they may publicly report the fact in their Annual Report."[539]

599. We heard that adequate resources were vital in ensuring the Judicial Commissioners were able to carry out their oversight and authorisation duties. JUSTICE commented that "whether that body succeeds in becoming a robust, transparent and accountable public facing body, which increases public confidence, will depend very much on its structure, powers and resources."[540] Privacy International told us that: "ensuring an appropriate level of resourcing for the IP Commission will be crucial in enabling the public and Parliament to ensure surveillance powers are properly used."[541] Sir Mark Waller, the Intelligence Services Commissioner, told us he did not think it appropriate for the Home Secretary to make decisions about the resources available to the Judicial Commissioners. Sir Mark emphasised that although the Secretary of State's control of the "purse strings" would not affect the decisions Judicial Commissioners made, inadequate resources would have a negative impact on their "ability to do the job."[542] Sir Stanley Burnton, Interception of Communications Commissioner, told us it was inappropriate for the "person who is being monitored in a sense to be the person who decides on the resourcing of the office."[543] Lord

536 Written evidence from Access Now et al. (IPB0109)
537 Written evidence from the Interception of Communications Commissioner's Office (IPB0101)
538 Clause 176(2)
539 Home Office, *Draft Investigatory Powers Bill: Explanatory Notes*, Cm 9152, November 2015, para 409
540 Written evidence from JUSTICE (IPB0148)
541 Written evidence from Privacy International (IPB0120)
542 Q 45 (Sir Mark Waller)
543 Q 56 (Sir Stanley Burnton)

EMBARGOED until 09.30 on 11 February 2016

Judge, the Surveillance Commissioner, agreed saying "if we are going to supervise the Home Secretary we must not answerable to him or her for the money."[544]

600. We heard from several witnesses that the new system was likely to be significantly more expensive than the current oversight structure due to the increase in functions the Judicial Commissioners are required to fulfil. Lord Judge told us:

> "If you have the same number of commissioners I have, which is six plus me plus three assistant commissioners, that is ten before you start. If Parliament enacts a system in which there is authorisation for everything in advance, it is going to take a lot more people. It will cost a lot more. We can either do it on the cheap or spend more money … Yes, it will cost a lot more."[545]

601. Sir Stanley Burnton agreed that significant numbers of staff would be needed:

> "in order properly to run the system, there are going to be something like eight judicial commissioners, which is quite a lot of staff. They must be backed up with appropriate staff, with the kind of skills my office now has but more widely available. There will be more inspectors, who must be appropriately qualified. You are looking at significant sums of money."[546]

602. We heard proposals for a number of alternative funding structures. The Bar Council suggested that the Home Office could propose a budget for the Judicial Commissioners which would then be examined and agreed by a Parliamentary Committee.[547] The Equality and Human Rights Commission also recommended a "role for Parliament" in determining the Judicial Commissioner's budget.[548] Sir Stanley Burnton and Lord Judge both supported direct negotiation between the Investigatory Powers Commissioner and the Treasury.[549] In New Zealand the Inspector-General of Intelligence and Security receives a fixed percentage of the spend on intelligence and policing.[550] Jo Cavan, the Head of the Interception of Communications Commissioner's Office, thought that that model could work here and observed "our percentage would no doubt be significantly lower than the percentage in New Zealand, because of the larger scale of our intelligence agencies, in particular the bulk collection we do, in comparison to New Zealand."[551]

603. In the United Kingdom, Estimates for the public service are normally laid before the House of Commons by the Treasury. There are four statutory bodies whose financial independence is enhanced by having their Estimates laid formally before the House of Commons by the Speaker (in the case of the Estimates for the Electoral Commission, House of Commons: Administration and for the Independent Parliamentary Standards Authority) or by the Chair of the Public Accounts Commission (for the National Audit Office). The spending of each of these four bodies out of the public money voted by Parliament is scrutinised by a statutory parliamentary committee. This model of statutory

EMBARGOED until 09.30 on 11 February 2016

544 Q 57 (Lord Judge)
545 Q 56 (Lord Judge)
546 Q 56 (Sir Stanley Burnton)
547 Written evidence from the Bar Council (IPB0134)
548 Written evidence from the Equality and Human Rights Commission (IPB0136)
549 Q 57 (Sir Stanley Burnton and Lord Judge)
550 Written evidence from Cheryl Gwyn (IPB0158)
551 Q 58 (Jo Cavan)

independence combined with parliamentary scrutiny is one possible approach to financial independence from direct Treasury control.[552]

604. ***We believe it is inappropriate for the Home Secretary alone to determine the budget of the public body which is monitoring her exercise of surveillance powers. The Government may want to consider a role for Parliament in determining the budget. (Recommendation 56)***

Power to modify the functions of the Judicial Commissioners

605. Clause 177 of the draft Bill gives the Home Secretary the power to "modify the functions" of the Judicial Commissioners through secondary legislation. The Explanatory Notes states that the reasons for the provision is to allow "a level of flexibility about the role of the Commissioner to ensure that it can be modified and adapted to fit with the work that needs to be overseen." The Explanatory Notes also comment that the changes would only occur with the consent of both Houses of Parliament.[553]

606. The Law Society of Scotland said that the effect of Clause 177 when read with Clause 197(1)(c) was to create a power to modify that was "exceptionally wide and draconian "effectively amounting to 'Henry VIII powers'." It noted that "There is no obligation to consult before making such modifications and there is no apparent oversight to ensure there is no excessive dilution of privacy rights. Also, it would appear there is no reasonable restriction on how the powers may be exercised."[554] JUSTICE also criticised the provision for its breadth and emphasised the negative impact of the provision on the perceived independence of the Judicial Commissioners. JUSTICE told us that the "limited capacity for Parliamentary scrutiny of secondary legislation makes this power inappropriate."[555] Amnesty International also criticised the provision for being an "extraordinarily wide power" and echoed concerns over the impact on the independence of the Judicial Commissioners.[556] Martin Chamberlain QC observed that the breadth of the proposed power meant it could be used "to alter the test that a judicial commissioner has to apply when considering or reviewing the issue of a warrant."[557]

607. Peter Carter QC suggested that limiting the power to modify the Judicial Commissioners functions so that it did not apply to the authorisation, renewal or continuation of warrants would counter some of the concerns expressed about its breadth.[558] Both JUSTICE and Amnesty submitted that the power to modify should be confined to primary legislation allowing full scrutiny by both Houses of Parliament of the need for and effect of any change.[559]

608. **Clause 177 contains a power for the Home Secretary to modify the functions of the Judicial Commissioners. While we recognise the concerns of some of our witnesses, we believe such a power is appropriate as we have every confidence such a power would only be exercised responsibly by the Secretary of State.**

552 House of Commons Administration Act 1978; National Audit Act 1983: Political Parties, Elections and Referendums Act 2000; Parliamentary Standards Act 2009, Schedule 1, paragraph 22
553 Home Office, *Draft Investigatory Powers Bill: Explanatory Notes*, Cm 9152, November 2015, para 410
554 Written evidence from the Law Society of Scotland (IPB0128)
555 Written evidence from JUSTICE (IPB0148)
556 Written evidence from Amnesty International UK (IPB0074)
557 Q 195 (Martin Chamberlain QC)
558 Q 195 (Peter Carter QC)
559 Written evidence from JUSTICE (IPB0148) and Amnesty International UK (IPB0074)

EMBARGOED until 09:30 on 11 February 2016

Impact of authorisation and oversight functions being exercised by the same body

609. The draft Bill provides that the Judicial Commissioners carry out both authorisation of warrants and oversight of the bodies applying for and exercising the powers granted by the warrants. This approach was heavily criticised by many of our witnesses.[560] The Interception of Communications Commissioner's Office said the dual function of the Judicial Commissioners could present a problem if "serious questions" arose over the "appropriateness" of a warrant in a particular case which required "proper investigation."[561] Much of the criticism focused on the public perception of the Judicial Commissioners' independence. The Information Commissioner told us that there must be no impression the Judicial Commissioners were "'marking their own work'" or the oversight role would be "compromised".[562] JUSTICE thought that "conflation" of functions reduced the "objective independence" of the Judicial Commissioners and potentially undermined the effectiveness of the "IPC model."[563]

610. We were told by the Open Rights Group that "similar arrangements" to those proposed by the draft Bill had been criticised by the European Court of Human Rights in a recent case for raising doubts about independence.[564]

611. The Home Secretary said she recognised the concerns expressed by our witnesses. Mrs May told us that it was expected that the Judicial Commissioner would keep their authorisation and oversight functions separate: "There will be two functions and, therefore, two sets of people within the Investigatory Powers Commissioner and that office—those who are undertaking the authorisation process and those who are undertaking the inspection process."[565] Mrs May anticipated some benefits from the "ability of [Commissioners] to interact, to understand some of the issues of practice" but expressed confidence in the Judicial Commissioners to "fiercely defend their independence" and the separate nature of their functions.[566]

612. **While we accept that the Judicial Commissioners must not be perceived as overseeing their own work, we do not think this is an insurmountable problem. We agree with the Home Secretary that the senior judges who will act as Judicial Commissioners will be well aware of the need to separate the authorisation and oversight functions with which they are entrusted. We emphasise that there needs to be a clear delineation of functions within the Judicial Commissioners in order to ensure public confidence in the independence and impartiality in the exercise of the Commissioners' oversight functions.**

EMBARGOED until 09:30 on 11 February 2016

560 For example, written evidence from Amnesty International UK (IPB0074), Cian C Murphy and Natasha Simonsen (IPB0096), Privacy International (IPB0120) and Liberty (IPB0143)

561 Written evidence from the Interception of Communications Commissioner's Office (IPB0101)

562 Written evidence from the Information Commissioner's Office (IPB0073)

563 Written evidence from JUSTICE (IPB0148)

564 Written evidence from Open Rights Group (IPB0108), European Court of Human Rights *Zakharov v Russia* (2015) application no. 47143/06

565 Q 282 (Theresa May MP)

566 Q 282 (Theresa May MP)

Error-reporting and notification

613. Clause 171 provides that the Investigatory Powers Commissioner must inform a person about any "serious error"[567] when the Investigatory Powers Tribunal agrees the error is serious and that it is in the "public interest for the person concerned to be informed of the error."[568] The error must be a "relevant error", one which concerns a public authority's breach of obligations imposed by the Bill or Code of Practice issued under Schedule 6 of the Bill.[569] A "serious error" is defined as a "relevant error" which the IPC and the IPT agree "has caused significant prejudice or harm" to the individual concerned.[570] The draft Bill excludes a breach of an individual's Convention rights from being a "serious error" where there has been no further harm.[571] When making a decision on whether a person should be informed of a serious error the IPT must consider whether informing that person would be prejudicial to national security; the prevention or detection of serious crime; the economic well-being of the United Kingdom, or the continued discharge of the functions of any of the the security and intelligence agencies.[572] Numbers of relevant and serious errors must be published in the Investigatory Powers Commissioner's annual report together with the number of people informed of serious errors.[573] In 2014, the Interception of Communications Commissioner recorded 998 errors that were reported to his office.[574]

614. The Bingham Centre for the Rule of Law told us that the approach in the draft Bill to error-reporting and notification was a matter of "profound concern":

> "We accept fully that there will be circumstances where a person has suffered significant prejudice or harm but that there will be good reasons (eg, national security) why they should not be notified, and it is right that the legislation provides for that. However, it is entirely inappropriate that the legislative presumption is against notification and that the legislation does not provide for notification at a future point when there are no longer reasons for secrecy. The rule of law requires access to justice, and this means that a person who is wronged should have an effective right to a remedy. This is especially so when that wrong has been at the hands of the state, and when the wrong has resulted in significant prejudice or harm."[575]

615. The Interception of Communications Commissioner's Office (IOCCO) told us that the provisions in Clause 171 were weaker than the current "well established" powers on error-reporting because it requires the agreement of the Investigatory Powers Tribunal to inform a person of an error. The approach adopted by the draft Bill "interferes with, dilutes and limits significantly the very well established function of the IOCCO to identify and investigate errors and of the Interception Commissioner to make determinations on errors and, where relevant, to inform individuals affected."[576] Dr Tom Hickman told us

567 Clause 171(1)
568 Clause 171(2)(ii)
569 Clause 171(11)
570 Clause 171(3)
571 Clause 171(4)
572 Clause 171(5)
573 Clause 171(10)
574 The Interception of Communications Commissioner, *Report of the Interception of Communications Commissioner*, March 2015
575 Written evidence from the Bingham Centre for the Rule of Law (IPB0055)
576 Written evidence from the Interception of Communications Commissioner's Office (IPB0101)

EMBARGOED until 09:30 on 11 February 2016

that there were no reasons for the reduction in the power of the oversight body to report errors, the current oversight bodies had operated their powers in this area without raising any concern.[577]

616. The requirement that an error cause "significant prejudice or harm" was criticised for being "a very high bar."[578] JUSTICE agreed describing the test as disproportionate and "inappropriately" high.[579] IOCCO said the test was "extremely high".[580] It noted that the test conflicted with the test for applying to the IPT where an applicant only has to show that their Convention rights may have been breached by a public authority. The IOCCO was also concerned that the test did not take into account the egregiousness of the conduct that led to the error and focused solely on the consequences.[581]

617. The test was also criticised for being poorly defined. The Law Society of Scotland told us that "no definition [is] provided for 'error' or 'serious error'. In the absence of a definition, these may be defined either widely or narrowly."[582] Privacy International said "what is considered "serious" needs further explanation, and what the public interest test will be is not clearly defined."[583] The IOCCO raised the practical point that the Investigatory Powers Commissioner and the IPT may have difficulties determining whether "serious harm or prejudice" if they are unable to contact the person in question,[584] and Amnesty International UK noted that the decision-makers would have no access to any "independent evidence" on this point.[585]

618. Both JUSTICE and Human Rights Watch argued that a breach of Convention rights should be an adequate reason for informing a person of an error so they are able to exercise their right to seek redress.[586] The IOCCO did not commit itself to a specific test but noted that a breach of some Convention rights are serious in and of themselves such as the rights to life, liberty and the protection against inhuman and degrading treatment.[587] An alternative test, proposed by Open Intelligence, would require the reporting of errors to individuals as a matter of course "unless there are significant reasons not to do, such as prejudicing an ongoing or planned operation/investigation".[588]

619. We heard from witnesses who called for a system of notification. This would require that a person who had been the subject of surveillance is informed of the fact "(and the grounds for it and materials selected, as well as potential remedies) as soon as this may be done without jeopardising the legitimate purpose of the surveillance."[589] Amnesty International UK told us that this approach is a "necessary requirement under international human rights law". McEvedys Solicitors agreed and said "A monitoring scheme will not be 'in accordance with the law' if it fails to ensure that persons who are monitored are

577 Written evidence from Dr Tom Hickman (IPB0039)
578 Written evidence from Privacy International (IPB0120)
579 Written evidence from JUSTICE (IPB0148)
580 Written evidence from the Interception of Communications Commissioner's Office (IPB0101)
581 *Ibid.*
582 Written evidence from the Law Society of Scotland (IPB0128)
583 Written evidence from Privacy International (IPB0120)
584 Written evidence from the Interception of Communications Commissioner's Office (IPB0101)
585 Written evidence from Amnesty International UK (IPB0074)
586 Written evidence from JUSTICE (IPB0148) and Human Rights Watch (IPB0123)
587 Article 2, 5 and 3 of the European Convention on Human Rights, respectively
588 Written evidence from Open Intelligence (IPB0066)
589 Written evidence from Amnesty International UK (IPB0074)

EMBARGOED until 09:30 on 11 February 2016

notified of the surveillance (if only ex post facto), see Assn. for European Integration and Human Rights & Ekimdzhiev v Bulgaria."[590]

620. In *A Question of Trust*, David Anderson QC recommended that the Judicial Commissioners be given the power to report errors to individuals where they may be entitled to compensation and subject to a duty not to disclose anything that would be damaging to national security or prejudice ongoing operations.[591]

621. ***Clause 171 changes the existing powers of the relevant commissioners to report errors in the use of surveillance powers to the individuals affected by raising the applicable test and requiring the involvement of the Investigatory Powers Tribunal in making the decision. This approach is cumbersome and unnecessary given there are no concerns over the way the current oversight bodies have used their powers of error-reporting. We recommend that the Investigatory Powers Commissioner exercise the error-reporting power alone, without reference to the Investigatory Powers Tribunal. (Recommendation 57)***

622. ***We recommend that the Government should review the error-reporting threshold in light of the points made by witnesses. (Recommendation 58)***

Powers and duties of the Judicial Commissioners

623. We heard a number of observations, criticisms and endorsements of the draft Bill's approach to the powers and duties of the Judicial Commissioners. We review these here and where appropriate provide our own conclusions.

Constraint on Judicial Commissioners

624. Clause 169(5) provides that in exercising the functions contained in the draft Bill a Judicial Commissioner must not act in a way that is contrary to the public interest or prejudicial to national security, the prevention or detection of serious crime or the "the economic well-being of the United Kingdom." Clause 169(7) limits the duties imposed by subclauses 169(5) and (6) to the oversight functions of the Judicial Commissioners.

625. Amnesty International UK criticised the "very broad drafting" of these subclauses, which do not define many of the terms they contain. This approach "lacks the required clarity of the law for such a serious provision." The breadth and vague nature of the subclauses was such that they had the potential to jeopardise the effectiveness of the Judicial Commissioners' oversight.[592] McEvedys Solicitors agreed and suggested that the Judicial Commissioners must consider proportionality at the same time as the other matters detailed in the subclauses.[593]

626. ***It should be made clear in the duties laid on the Judicial Commissioners in subclauses 169(5) and (6) that they must comply with those duties in a proportionate manner. The subclauses are drafted in very broad and uncertain terms which have the potential to impact upon the work of Judicial Commissioners in unintended ways. Public confidence in the independence of the Judicial Commissioners requires clarity***

590 Written evidence from McEvedys Solicitors & Attorneys Ltd (IPB0138)
591 David Anderson QC, *A Question of Trust: Report of the Investigatory Powers Review*, 2015, Recommendation 99
592 Written evidence from Amnesty International UK (IPB0074)
593 Written evidence from McEvedys Solicitors & Attorneys Ltd (IPB0138)

EMBARGOED until 09:30 on 11 February 2016

and transparency in both powers and duties. We recommend that Clauses 169(5) and (6) should be re-drafted to protect the Judicial Commissioners' independence and to ensure the Judicial Commissioners are not constrained from providing effective oversight. (Recommendation 59)

Whistle blowers and the Judicial Commissioners

627. The Interception of Communications Commissioner's Office suggested that the Bill should include "an explicit provision for CSPs and staff within public authorities to refer directly to the Investigatory Powers Commission any complaint or concern they have with conduct proposed or undertaken, or any matter on which they require clarification."[594] Graham Smith thought that service providers should be able to bring "a legal interpretation asserted against them" to the attention of the Judicial Commissioners who would then be able to inform other service providers by making the interpretation public.[595] More controversially, we also heard a suggestion that the Bill address whistle-blowing in the security and intelligence agencies. The relationship between potential whistle-blowers in the agencies and the Judicial Commissioners received attention from some witnesses. The nature of surveillance powers inevitably means that, if they are misused or misapplied, individuals who are aware of any misconduct may not only be legally barred from making their concerns public but may in any event be loath to do so given the potential assistance disclosures could give to people who pose a threat to national security.

628. Public Concern at Work, a charity which runs a confidential helpline for potential whistle blowers, noted that the channels through which intelligence service personnel could report misconduct were uncertain. While evidence given to the Intelligence and Security Committee may not be used in civil or criminal proceedings unless it is given in bad faith, the position for anyone contacting the ISC but not giving evidence is not protected. Public Concern at Work suggested that where a whistle-blower's concerns fall within internationally recognised specified categories of wrongdoing or malpractice[596] they should be able to report them to the Judicial Commissioners without being at risk of prosecution for breaching the Official Secrets Act.[597]

629. ***We recommend that the Bill should contain an explicit provision for Communication Service Providers and staff in public authorities to refer directly to the Judicial Commissioners any complaint or concern they may have with the use of the powers under the Bill or any request for clarification on the use of those powers. Where clarification is provided the Judicial Commissioners will need to have the power to make that information public should it be appropriate in the circumstances. This will enable better compliance with the provisions of the Bill and will help to reduce costs. (Recommendation 60)***

630. ***We recommend that members of the security and intelligence agencies should be able to contact the Investigatory Powers Commissioner with concerns over the misuse of surveillance powers without being at risk of prosecution for breaching the Official Secrets Act. The Investigatory Powers Commissioner should then have discretion whether to***

594 Written evidence from the Interception of Communications Commissioner's Office (IPB0101)
595 Written evidence from Graham Smith (IPB0126)
596 As set out in Open Society Foundations, *Global Principles on National Security and the Right to Information (Tshwane Principles)*, 12 June 2013
597 Written evidence from Public Concern at Work (IPB0077)

EMBARGOED until 09:00 on 11 February 2016

exercise his or her power to initiate an inquiry into the allegations. We recognise that there may be wider concerns over the role of whistle-blowers in this area. This is a matter which requires consultation and therefore this is not the appropriate Bill in which those wider concerns should be taken forward. (Recommendation 61)

Legal advice and access

631. The Anderson report recommended that the Judicial Commissioners have both an "in-house legal presence" and "one or more" part-time "security-cleared standing counsel". Counsel's function would be, on request:

- to give advice on recent developments in the law;
- to advise ISIC on possible legal vulnerabilities in the arrangements whose operation it reviews;
- to advise (at the request of the Judicial Commissioners) in relation to applications for warrants or requests for authorisations on proposed communications data authorisations;
- to assist with the legal aspects of formulating guidance and contributing to Codes of Practice; and
- by these means to help ISIC ensure that the activities it authorises, audits or reviews are lawful, and that the public authorities it oversees have due warning of legal difficulties.[598]

632. We asked the current Commissioners whether they thought the Judicial Commissioners would require legal assistance. Lord Judge, the Chief Surveillance Commissioner, told us he thought they would because the law in this area is "extremely complex":

> "RIPA is a dreadful piece of legislation. I say that with some strength of feeling, having had to try to understand it. Why do judges need a legal adviser? For that reason: to say it could be any one of 17 possible interpretations, rather than the five you thought you had. More importantly, in this system, from time to time you need advice."[599]

633. The Bingham Centre for the Rule of Law thought that a special advocate would be required to advise the Judicial Commissioner when an application for a warrant or authorisation was "novel or raises especially contentious issues (including where the possible interpretation of a statute which would see an expansion of powers that differs from what is apparent on the face of the legislation)".[600] Dr Tom Hickman agreed "one can envisage their use routinely in controversial cases on the boundaries of 'national security', in cases involving journalists and lawyers and major operations, in cases which rely on a broad meaning of the Act or which test key provisions, and in many other cases in which a JC perceives some issue on which he or she would appreciate contrary argument being put forward."[601] Amnesty International UK said that it was "highly desirable to enhance

598 David Anderson QC, *A Question of Trust: Report of the Investigatory Powers Review*, 2015, Recommendation 110 and written evidence from David Anderson QC (IPB0152)
599 Q 52 (Lord Judge)
600 Written evidence from Bingham Centre for the Rule of Law (IPB0055)
601 Written evidence from Dr Tom Hickman (IPB0039)

EMBARGOED until 09:30 on 11 February 2016

the adversarial nature" of the authorisation process to ensure human rights was properly considered.[602]

634. ***The law in this area is complex and developing. Judicial Commissioners will have to make decisions without the benefit of adversarial argument. We agree with the Independent Reviewer of Terrorism that Judicial Commissioners must have access to both in-house legal expertise and, on request, security-cleared independent counsel to assist them in both the authorisation and oversight functions of their role. (Recommendation 62)***

Technical advice and access

635. The Interception of Communications Commissioner's Office told us that effective oversight required that the Judicial Commissioners must be "provided with access to technical systems to assist audits, inspections and inquiries to be carried out. Any new technical systems (e.g. secure automated CSP disclosure systems, the request filter, workflow systems managing applications and authorisations) must be developed with oversight and audit functions in mind."[603] Such a mandate would contribute to compliance with the European Convention on Human Rights by assisting the Judicial Commissioners in providing effective oversight.[604]

636. Sir Mark Waller, the Intelligence Services Commissioner, told us that the functions covered by his office did not need "a great deal of technical expertise."[605] Lord Judge told us, however, that in his view the Judicial Commissioners would require "one or two people with serious expertise in technology" in order to fulfil their functions.[606] David Anderson QC said that technical expertise would enhance the ability of the Judicial Commissioners to fulfil their oversight function noting "I have very high regard for what the commissioners have done, but I remarked in my report that it was not the courts, commissions or committees of London that disclosed to the British people what was going on; it was the revelations that originally came from Mr Snowden. That is not the way it should be."[607]

637. ***We recommend that the Judicial Commissioners should have a legal mandate to access all relevant technical systems required to ensure effective oversight of the powers contained in the Bill. This mandate should appear on the face of the Bill. (Recommendation 63)***

638. ***We recommend that the Judicial Commissioners should have access to technical expertise to assist them in fulfilling their authorisation and oversight functions. (Recommendation 64)***

Other powers and duties

639. Clause 172(3) requires the Judicial Commissioners to consult the Home Secretary before advising or providing information to a public authority "or any other person" if the

602 Written evidence from Amnesty International UK (IPB0074)
603 Written evidence from the Interception of Communications Commissioner's Office (IPB0101)
604 For example, European Court of Human Rights *Zakharov v Russia* (2015) application no. 47143/06
605 Q 41 (Sir Mark Waller)
606 Q 52 (Lord Judge)
607 Q 70 (David Anderson QC)

EMBARGOED until 09:30 on 11 February 2016

Judicial Commissioner believes providing the advice or information may be contrary to the public interest or prejudicial to national security, the prevention or detection of serious crime, the economic well-being of the United Kingdom, or the continued discharge of the functions of any public authority whose activities include activities that are subject to review by the Investigatory Powers Commissioner. JUSTICE expressed concern that the drafting of this clause could require the Judicial Commissioners to consult the Home Secretary before advising the Investigatory Powers Tribunal on a point of law, and that this could mar the Judicial Commissioners' independence.[608] It is unclear what purpose the application of the duty to consult the Home Secretary would serve when the issue is legal advice to a court and it appears this may be an unintended and inappropriate consequence of the drafting.

640. ***The Judicial Commissioners should be able to communicate with the Investigatory Powers Tribunal on a point of law without consulting the Home Secretary. Clause 172(3) should be redrafted to reflect this. (Recommendation 65)***

641. We were told that the draft Bill does not contain a power for the Judicial Commissioners to refer matters to the Investigatory Powers Tribunal for consideration. The RUSI report on surveillance recommended that the Judicial Commissioners have a statutory right to refer cases to the IPT where they find a material error or arguable illegality or disproportionate conduct.[609] The Interception of Communication Commissioner's Office agreed. It said that this power should be "express" to allow the two bodies to carry out their respective roles "the Investigatory Powers Commissioner as an audit and investigation body" and the Investigatory Powers Tribunal as "the means by which individuals can seek remedy where they believe they have been a victim of unlawful action under RIPA or human rights infringements."[610] JUSTICE added that this power "could be particularly useful where an issue affects a group or class of individuals unlikely to pursue an individual claim before the Tribunal; or in circumstances where the interpretation of the law or its application to a new practice may be in doubt."[611]

642. ***The Judicial Commissioners should be able to make a direct reference to the Investigatory Powers Tribunal where they have identified unlawful conduct following an inspection, audit, investigation or complaint. (Recommendation 66)***

643. Clause 174(2) sets out the mandatory requirements of the Investigatory Powers Commissioner's annual report for the Prime Minister. The Information Commissioner told us that the report must contain information on the "results achieved" from the use of investigatory powers. "This is essential to judging whether measures are necessary", the Information Commissioner said, and would assist in "effective post-legislative scrutiny."[612]

644. The Information Commissioner also suggested that "transparency would be … aided" if the IPC's annual reports contained figures on the number of warrants or notices that have been served at one time, although without the names of the organisations involved:

EMBARGOED until 09:30 on 11 February 2016

608 Written evidence from JUSTICE (IPB0148)
609 Royal United Services Institute (RUSI), *A Democratic Licence to Operate: Report of the Independent Surveillance Review*, July 2015, Recommendation 16
610 Written evidence from the Interception of Communications Commissioner's Office (IPB0101)
611 Written evidence from JUSTICE (IPB0148)
612 Written evidence from the Information Commissioner's Office (IPB0073)

"Expanding the breadth of the IPC's reports will also be a welcome step towards further increased transparency, a prerequisite for helping maintain public trust and confidence."[613]

645. When considering the arguments for an expanded annual report we noted that the draft Bill gives the Prime Minister the power to redact the Investigatory Powers Commissioner's reports, after consultation with the Investigatory Powers Commissioner. The redacted report is then laid before Parliament.[614] The "wide discretion" available to the Prime Minister under this provision caused Amnesty International UK some concern.[615]

646. ***The Investigatory Powers Commissioner's annual report must include information about the impact, results and extent of the use of powers in the Bill so effective public and parliamentary scrutiny of the results of the powers can take place. (Recommendation 67)***

647. ***The Investigatory Powers Commissioner should be able to inform the Intelligence and Security Committee if he or she is unhappy about the use of the Prime Minister's power to redact his annual report. (Recommendation 68)***

Issuing guidance

648. The Anderson report recommended that the Judicial Commissioners should have the power to issue guidance to public authorities applying for warrants and authorisations. The guidance would "supplement the new law and any codes of practice issued under it and … should be published where the constraints of national security permit."[616]

649. ***We recommend that the Judicial Commissioners should have the power to develop guidance to public authorities to assist them in applications seeking to use investigatory powers. This will help applicant bodies to formulate focused applications saving time and resources. Where the constraints of national security allow, the guidance should be published in the interests of public transparency and foreseeability. (Recommendation 69)***

The Investigatory Powers Tribunal

Power of appeal

650. The Investigatory Powers Tribunal does not have a route of appeal beyond an application to the European Court of Human Rights on a point of human rights law.[617] Clause 180 creates a new right of appeal from the Investigatory Powers Tribunal. An appeal may be made if it would raise an important point of principle or practice, or if there is another compelling reason for granting leave.[618] An appeal may only be made with the leave of the Investigatory Powers Tribunal or the court which would have jurisdiction to hear the appeal—the Court of Appeal in England and Wales or a court specified in regulations by the Home Secretary.[619]

613 *Ibid.*
614 Clause 174(4)
615 Written evidence from Amnesty International UK (IPB0074)
616 David Anderson QC, *A Question of Trust: Report of the Investigatory Powers Review*, 2015, Recommendation 84(f)
617 Regulation of Investigatory Powers Act 2000 sections 65–68
618 Clause 180(4)
619 Clause 180

EMBARGOED until 00:30 on 11 February 2016

651. The introduction of a right of appeal, which was recommended by both the Anderson and RUSI reports,[620] was welcomed by witnesses.[621] The restrictive nature of the right of appeal was though the subject of negative comment. Martin Chamberlain QC told us:

> "This restrictive test is modelled on the test for second appeals in rule 52.13(2) of the Civil Procedure Rules 1998. But this is a first appeal. It is unclear why such a restrictive test is considered necessary here. There is no similar restriction on appeal from the Special Immigration Appeals Commission (see s. 7 of the SIAC Act 1997, which confers a right of appeal "on any question of law material to [the] determination")."[622]

652. Matthew Ryder QC said the way the right to appeal was drafted was "at best, unhelpful" because it could constrain the Court of Appeal to refuse leave to appeal "even if it considers there are arguable grounds that the Investigatory Powers Tribunal made a significant error of law" because that error of law did not raise an "'important point of principle and practice'".[623] Mr Ryder described such an outcome as "unconscionable" as identified errors of law would be without remedy or appeal. In *A Question of Trust*, David Anderson QC recommended that an appeal from the Investigatory Powers Tribunal should be available for an error of law.[624]

653. JUSTICE raised two concerns over the proposed appeal process. The first was that the right to appeal only seems to apply to a final judgment not to interim legal decisions during proceedings. "This could lead to unfairness and wasted resources as proceedings may continue to a full determination on the basis of an error in law, only to result in an appeal at a later stage." JUSTICE also queried the decision to provide that an appeal in Scotland and Northern Ireland would be heard by a court specified by the Home Secretary: "delegation of this kind is inappropriate. Routes of appeal should be specified on the face of the Bill."[625]

654. ***We recommend that the right of appeal from the Investigatory Powers Tribunal in Clause 181 should be amended to include cases where there has been an error of law to prevent injustice as a matter of public policy and to satisfy the rule of law. (Recommendation 70)***

655. ***We recommend that rulings in the Investigatory Powers Tribunal should be subject to an interim right of appeal on the grounds of an error of law to save time and costs. (Recommendation 71)***

656. ***We recommend that the appeal route for Scotland and Northern Ireland should appear on the face of the Bill. It is unclear to us why there is not a specified route of appeal in Scotland and Northern Ireland nor what appellants in those parts of the United Kingdom are expected to do before the Home Secretary issues regulations on this issue. (Recommendation 72)***

620 Royal United Services Institute (RUSI), *A Democratic Licence to Operate: Report of the Independent Surveillance Review*, July 2015, Recommendation 14; David Anderson QC, *A Question of Trust: Report of the Investigatory Powers Review*, 2015, Recommendation 114

621 For example, written evidence from the Bingham Centre for the Rule of Law (IPB055) and Cian C Murphy and Natasha Simonsen (IPB0096)

622 Written evidence from Martin Chamberlain QC (IPB0133)

623 Written evidence from Matthew Ryder QC (IPB0142)

624 David Anderson QC, *A Question of Trust: Report of the Investigatory Powers Review*, 2015, Recommendation 99

625 Written evidence from JUSTICE (IPB0148)

EMBARGOED until 09:30 on 11 February 2016

Review of procedures and processes

657. Both the reviews carried out by the Independent Reviewer of Terrorism Legislation and the Royal United Services Institute (RUSI) recommended an overhaul of the Investigatory Powers Tribunal. RUSI recommended that "The Investigatory Powers Tribunal (IPT) should be as open as possible and proactively find ways that make its business less opaque to the public."[626] Mr Anderson observed that public confidence in the IPT was not encouraged by the fact that "1,673 complaints determined by the end of 2013, only 10 were upheld—five of them involving members of the same family, and none of them against the security and intelligence agencies."[627] The recommendations to review the IPT are not addressed by the draft Bill.

658. A number of witnesses complained that the Investigatory Powers Tribunal operated in an "opaque"[628] manner with a "bias towards secrecy".[629] Specific concerns were directed at the use of closed hearings, the lack of special counsel for claimants, the restrictions on disclosure and evidence and the limited reasons given to claimants even when they are successful.[630] Matthew Ryder QC told us that "any blanket prohibition on publicity of categories of IPT judgments (e.g. an absolute ban on providing any details of a finding against a complainant) is undesirable and should be reconsidered."[631] Rachel Logan of Amnesty International UK told us that the "sparse" judgement meant her organisation had "found very little out" from a case it won in the IPT.[632] Ms Logan also told us that Amnesty International UK had been unable to get an explanation for why it had initially been told that it had not been successful in that case, only to later be told that there had been a mistake, Amnesty International UK had won but the IPT had apparently confused the organisation with another claimant:[633]

> "That was following a hearing that supposedly was looking in the most detailed consideration at our rights and at particular communications that had been intercepted and whether that was lawful and proportionate. We asked, quite rightly, "How can this happen?", and asked for an open determination explaining how a mistake of this kind had been made. We received a very unsatisfactory response from the tribunal. Indeed, Parliamentary Questions have been asked about this by quite a few Members of the House—both Houses, in fact—seeking a Statement from the Secretary of State, asking whether other human rights organisations have been in the same position, and nothing has been forthcoming."[634]

659. Amnesty International UK concluded that the IPT's rules and procedures impaired the "essence of fair trial rights" and did not constitute an effective oversight body.[635]

EMBARGOED until 09.30 on 11 February 2016

626 Royal United Services Institute (RUSI), *A Democratic Licence to Operate: Report of the Independent Surveillance Review*, July 2015, Recommendation 11
627 David Anderson QC, *A Question of Trust: Report of the Investigatory Powers Review*, 2015, para 6.106
628 Written evidence from Cian C Murphy and Natasha Simonsen (IPB0096)
629 Q 203 (Rachel Logan, Amnesty International UK)
630 Written evidence from Open Intelligence (IPB0066), Amnesty International UK (IPB0074) and JUSTICE (IPB0148)
631 Written evidence from Matthew Ryder QC (IPB0142)
632 Q 203 (Rachel Logan, Amnesty International UK)
633 *Ibid.*
634 *Ibid.*
635 Written evidence from Amnesty International UK (IPB0074)

660. ***The Home Office should conduct a consultation and review of the powers and procedures of the Investigatory Powers Tribunal with the aim of improving openness, transparency and access to justice. (Recommendation 73)***

661. In its report, the Royal United Services Institute recommended that the IPT "should hold open public hearings, except where the Tribunal is satisfied that private or closed proceedings are necessary in the interests of justice or other identifiable public interest."[636]

662. Martin Chamberlain QC told us that the Investigatory Powers Tribunal had recognised in 2003 that as much of its proceedings must be held in public as possible.[637] To date such disclosure as was made as a result of the open hearings had been made with the consent of the intelligence agencies. Mr Chamberlain suggested that:

> "It would add to the credibility of the IPT as an oversight mechanism, and to its ability to contribute to compliance with Article 8 standards, if it were given express power to decide for itself whether material deployed before it should be made public and to what extent. In exercising this power, it would of course consider carefully any arguments made to it by the agencies that disclosure would be damaging to national security or another protected public interest, but it would ultimately have the function of deciding that question for itself."[638]

663. ***The Investigatory Powers Tribunal should have the power to decide whether its proceedings should be held in public. When making a decision on whether a hearing or part of a hearing should be open or not the Tribunal should apply a public interest test. (Recommendation 74)***

664. The IPT is not a "senior court" which means it is not able to make a declaration of incompatibility under section 4 of the Human Rights Act 1998. In *A Question of Trust*, David Anderson QC recommended that the IPT should have this capacity.[639] Both Liberty and JUSTICE supported this recommendation.[640]

665. Mr Anderson observed that his recommendation that the IPT be empowered to make a declaration of incompatibility was in based in part of the lack of an appeal from the IPT to a higher court which was able to make such a judgment. The draft Bill introduces a right of appeal but it is drafted in restrictive terms and requires that the appeal engage an "important point of principle and practice".[641] Allowing the IPT to make a declaration of incompatibility will improve access to justice in this area.

666. ***The Investigatory Powers Tribunal should be able to make a declaration of incompatibility under the Human Rights Act. (Recommendation 75)***

EMBARGOED until 09:30 on 11 February 2016

636 Royal United Services Institute (RUSI), *A Democratic Licence to Operate: Report of the Independent Surveillance Review*, July 2015, Recommendation 12

637 Written evidence from Martin Chamberlain QC (IPB0133); Investigatory Powers Tribunal, Kennedy and Other Ruling, IPT/01/62& 77

638 Written evidence from Martin Chamberlain QC (IPB0133)

639 David Anderson QC, *A Question of Trust: Report of the Investigatory Powers Review*, 2015, Recommendation 115

640 Written evidence from Liberty (IPB0143) and JUSTICE (IPB0148)

641 Clause 180

The oversight landscape

667. As noted above, the draft Bill greatly simplifies the oversight landscape by replacing the three surveillance commissioners with one. We heard evidence, that further simplification could be undertaken. The Interception of Communications Commissioner's Office (IOCCO) said: "In our view there is still considerable room to revise the oversight provisions to simplify the oversight landscape, avoid overlaps and ensure consistency of decision making."[642] Other witnesses drew attention to the provisions in the draft Bill concerning the Information Commissioner. Open Intelligence said: "some oversight functions of the bill are still given to another body, the ICO. For completeness, the obligations under cl 182 should also be carried out by the IPC."[643] Vodafone commented:

> "at the moment, it appears that the Information Commissioner's Office, rather than the Investigatory Powers Commissioner, will be responsible for assessing some aspects of a provider's compliance. We fear that this bifurcated approach is likely to lead to a complexity and confusion, when what is needed is a simple and strong oversight regime."[644]

668. Virgin Media expressed similar concerns on the grounds that "the IPC … will have extensive audit rights and considerable knowledge of any infrastructure. We believe this is the best approach to ensure security of the retained data."[645]

669. The Information Commissioner told us that his role in auditing Communication Service Providers' infrastructure ensuring the security of retained data could be made easier if the draft Bill addressed a number of practical points such as ensuring the CSPs were obliged to cooperate with him and extending the criminal sanctions he and his staff faced if they revealed data they obtained in the course of an investigation to the ICO's communications with CSPs.[646]

670. ***We have heard evidence that there is potential for the further simplification of the oversight landscape. This would improve transparency, reduce overlaps and ensure consistency of decision-making which would all contribute to ensuring oversight of the powers contained in the Bill comply with international law standards. We recommend that the Home Office should carry out a review to identify areas in which further simplification of oversight could occur. (Recommendation 76)***

Privacy and Civil Liberties Board

671. The Committee notes that the Privacy and Civil Liberties Board, whose creation was authorised under section 46 of the Counter-Terrorism and Security Act 2015 has not yet been created by the Government. ***We call on the Government to outline its plans for the establishment of the Privacy and Civil Liberties Board. (Recommendation 77)***

EMBARGOED until 09:30 on 11 February 2016

642 Written evidence from the Interception of Communications Commissioner's Office (IPB0101)
643 Written evidence from Open Intelligence (IPB0066)
644 Written evidence from Vodafone (IPB0127)
645 Written evidence from Virgin Media (IPB0160)
646 Q 228 (Christopher Graham)

6 Remaining issues

The inadmissibility of intercept material as evidence

672. The draft Bill maintains the status quo which prohibits intercepted material from being used as evidence in court.[647] In his report, *A Question of Trust*, David Anderson QC addressed some of the reasoning for this and referred to the findings of the most recent review into this issue led by Sir John Chilcott.[648] In his response to the findings of Chilcott's review, the Security Minister at the time, James Brokenshire MP stated that allowing intercept as evidence would be too costly and the possible benefits would be outweighed by the potential risks.[649]

673. The Committee received evidence on this issue which again asks for the Government to reconsider its position.[650] As the Bar Council pointed out:

> "the Bill allows such material to be used in the tribunals set out in Schedule 3 (see section 42(1)), namely the IPT, [the Special Immigration Appeals Commission (SIAC)], etc. If the intercept material can be used in those tribunals, presumably predominantly to support the government's case, it is difficult to see why it cannot be used in non-closed proceedings, even if the process by which it has been obtained is not in evidence nor disclosed to the accused. There have now been numerous reports on this matter, and the use of it in closed proceedings only is unsatisfactory. The absolute prohibition on use of this material in certain cases of serious crime risks failure to do justice to victims and potential victims of e.g. modern slavery offences."[651]

674. This issue is further complicated, in the view of Big Brother Watch, by "the fact that evidence gained through equipment interference is permitted"[652] (see paras 300–305), making the "argument that the evidence from intercepting communications would reveal too much about the methods and work of the intelligence agencies [seem] nonsensical when it is permitted in a power which only recently has been avowed."[653]

675. ***The Committee recommends that the Government keeps the issue of the inadmissibility of intercept material as evidence under review and takes note of the significant perceived benefits of using such material as evidence. (Recommendation 78)***

Disclosure of intercept evidence to judges and prosecutors

676. Schedule 3 sets out some exceptions to Clause 42, and Clause 21 of Schedule 3 deals with disclosures to prosecutors and judges, with Clause 21(6) detailing who can be considered to be a relevant judge.

EMBARGOED until 09:30 on 11 February 2016

647 Clause 42
648 David Anderson QC, *A Question of Trust: Report of the Investigatory Powers Review*, 2015, paras 9.16–9.18
649 HC Deb, 17 December 2014, col 99WS
650 For example, written evidence from Big Brother Watch (IPB0007), Martin Chamberlain QC (IPB0133), the Bar Council (IPB0134), Liberty (IPB0143), JUSTICE (IPB0148)
651 Written evidence by the Bar Council (IPB0134)
652 Written evidence by Big Brother Watch (IPB0007)
653 *Ibid.*

677. The Committee received written evidence from HH Judge Peter Thornton QC, the Chief Coroner, proposing that this list be extended. He proposed that "the list of persons who are "a relevant judge" in paragraph 21 of Schedule 3 to the Bill be extended to include: retired judges of the High Court or retired Circuit judges who are under the age of 75."[654] This would be so that if a retired judge is nominated to conduct an investigation (including an inquest), he or she will be able to view relevant material. Without being able to do so, the investigation and inquest process may be incomplete. This would also include a judge who is nominated in the same way before retirement to conduct an investigation (including inquest) which continues after the judge's retirement age.

678. Additionally, "the Chief Coroner proposes that the list in paragraph 21 of Schedule 3 should also include a cadre of six senior coroners of England and Wales, selected by the Chief Coroner and approved by the Lord Chief Justice, who are under the age of 75. This cadre is necessary because more and more coroner investigations (including inquests) involve intelligence material. Where this arises, and it would not be necessary for a judge to be nominated to conduct the investigation (including inquest), the Chief Coroner could direct a senior coroner from the cadre to conduct the investigation (and inquest). The Chief Coroner could also arrange special training for the cadre of senior coroners."[655]

679. ***The Committee recommends that the Government should consider the Chief Coroner's proposals and engages further with him to come to a satisfactory agreement about which judges can be included in the list in Schedule 3. (Recommendation 79)***

Power to make consequential provision

680. The DPRRC in their memorandum on delegated powers highlight the power in Clause 201(2) to make consequential provision. They explained that:

> "Clause 201(2) confers a power on the Secretary of State by regulations to make such consequential provision as he or she considers appropriate. In common with many provisions of this kind, Clause 201(3) provides that this power may be exercised by amending or otherwise modifying provisions of primary or subordinate legislation."[656]

681. Firstly, they draw attention to the fact that this allows the Secretary of State to modify future enactments:

> "Clause 201(3) refers to "enactments" and it is clear from the way in which this expression is defined in Clause 195(1) that the powers conferred by Clause 201(3) include the power to amend or otherwise modify future enactments. While it is reasonable for there to be a need to amend past enactments to ensure that they fit with the provisions of the Bill, the same does not necessarily apply to future legislation which should be capable of taking account of the Bill's provisions when it is enacted. Accordingly, we would ordinarily expect a convincing case to be made in the memorandum for a power to use subordinate legislation to amend future primary legislation. In this case, the memorandum says nothing about why it is necessary to have the power to amend future enactments. Two

654 Written evidence by HH Judge Peter Thornton QC (IPB0026)
655 *Ibid.*
656 Memorandum from the House of Lords Select Committee on Delegated Powers and Regulatory Reform (see Appendix 3)

EMBARGOED until 09:30 on 11 February 2016

> precedents are given in paragraph 113 of the memorandum, but in neither case does the power include a power to amend future enactments. **We regard this aspect of the power as being inappropriate in the absence of a reasonable explanation for why it is needed.**"[657]

682. ***We agree with this conclusion of the DPRRC on the power in Clause 201 (2) to make consequential provision and recommend the deletion of powers to amend future enactments. (Recommendation 80)***

683. Additionally, the DPRRC draw attention to the negative procedure for modifications to a provision of primary legislation:

> "Regulations under Clause 201(2) are subject to the affirmative procedure where they amend or repeal a provision of primary legislation. The negative procedure applies in all other cases, including where the regulations otherwise modify a provision of primary legislation. Non-textual modification of primary legislation can however be used to make changes which are no less significant than textual amendments. **We have expressed the view, therefore, on a number of occasions—most recently in our reports on the Scotland Bill[658] and the Enterprise Bill[659]—that, as a matter of general principle, non-textual modifications of primary legislation should be subject to the same level of Parliamentary scrutiny as textual amendments, namely, the affirmative procedure.**"[660]

684. ***We agree with the DPRRC that the negative procedure for these powers is inappropriate and recommend that any modifications to primary legislation be subject to the super-affirmative resolution procedure. (Recommendation 81)***

Non-Technical Definitions

685. A number of issues have been raised about technical definitions in the draft Bill and these have been addressed under Chapter 3 (Capabilities) of this report.

686. Additionally, discussion around the definition of 'urgent' in relation to urgent warrants is discussed in paras 453–460.

687. A number of witnesses have also expressed concerns about the fact that other non-technical concepts of high importance are not defined by the draft Bill, and this section will examine some of these.

National Security

688. National security is given as a test of the necessity of an action for the following powers in the draft Bill:

EMBARGOED until 09:30 on 14 February 2016

657 *Ibid.*

658 Delegated Powers and Regulatory Reform Committee, *Scotland Bill; Trade Union Bill; Enterprise Bill; Draft Legislative Reform (Exempt Lotteries) Order 2016* (15th Report, Session 2015–16, HL Paper 64) paras 10 to 13

659 Delegated Powers and Regulatory Reform Committee, *Enterprise Bill [HL]: European Union Referendum Bill* (9th Report, Session 2015–16, HL Paper 42) paras 17 to 21

660 Memorandum from the House of Lords Select Committee on Delegated Powers and Regulatory Reform (see Appendix 3)

- Targeted interception warrants (Clause 14(3)(a))
- Targeted communications data authorisations (Clause 46(7)(a))
- Targeted equipment interference authorisation for the intelligence services (Clause 84(4)(a))
- Targeted equipment interference authorisations for the Chief of Defence Intelligence (Clause 87(1)(a))
- Targeted equipment interference warrants authorised by Chief Constables (Clause 89(7))
- Bulk interception warrants (Clause 107(1)(b))
- Bulk acquisition warrants (Clause 122(1)(a))
- Bulk equipment interference warrants (Clause 137(1)(b))
- Class bulk personal dataset warrants (Clause 153(3)(a))
- Specific bulk personal dataset warrants (Clause 154(5)(a))
- National security notices (Clause 188).

689. National security is also given as a valid reason for the following actions:

- Removing the need for a designated senior officer authorising a communications data request to be independent of the investigation operation (Clause 47(3)(a))
- Removing the need for an applicant for communications data to consult a SPoC (Clause 60(3)(a)).

690. Witnesses have pointed out that the term "national security", which can be used to justify so many of the actions provided for in the draft Bill, is never defined anywhere in the Bill.[661] Rachel Logan from Amnesty International UK said, "just recently, a decision by the Grand Chamber in Strasbourg, I think last week, said that it is important to have tighter definitions than just "threats to national security when we talk about warrants of this kind."[662]

691. ***The Committee recommends that the Bill should include a definition of national security in order to provide clarity to the circumstances in which these warrants can be issued. (Recommendation 82)***

Economic well-being

692. Similarly, "the economic well-being of the UK so far as those interests are also relevant to the interests of national security" is given as a test of the necessity of an action for the following powers in the draft Bill:

- Targeted interception warrants (Clause 14(3)(c))

661 See, for example, Q 77 (Professor Ross Anderson) and written evidence from Annie Machon (IPB0064)
662 Q 203 (Rachel Logan, Amnesty International UK)

EMBARGOED until 09:30 on 11 February 2016

- Targeted communications data authorisations (Clause 46(7)(c))
- Targeted equipment interference authorisation for the intelligence services (Clause 84(4)(c))
- Bulk interception warrants (Clause 107(2)(b))
- Bulk acquisition warrants (Clause 122(2)(b))
- Bulk equipment interference warrants (Clause 137(2)(b))
- Class bulk personal dataset warrants (Clause 153(3)(a))
- Specific bulk personal dataset warrants (Clause 154(5)(a)).

693. Again, witnesses felt this term was too vague to justify some of the powers it authorises. Professor John Naughton and Professor David Vincent suggested that it would be "appropriate that the purpose of "economic well-being" should receive critical scrutiny by Parliament."[663]

694. Lord Carlile, while opposed to a statutory definition, did highlight the need for some clarity:

> "there should be greater understanding in this context of 'safeguarding the economic well-being of the UK'. Whilst I am opposed to a statutory definition, the Committee would be entitled to look for more clarity as to the process whereby this criterion is certified, and who is involved. It would be reasonable for HM Treasury to be required operationally in each case to certify that the issues under consideration reached the high standard implied by the test."[664]

695. The UN Special Rapporteurs were concerned that "ambiguous terms such as "economic well-being", [heighten] the risk of excessive and disproportionate interception."[665]

696. ***The Committee recommends that the Bill should include a definition of economic well-being in order to provide clarity to the circumstances in which these warrants can be issued. (Recommendation 83)***

Publication of codes of practice

697. Above we have demonstrated the importance of codes of practice in containing much of the detail about the way the powers in the draft Bill will be exercised. This point was also underlined recently by the House of Commons Science and Technology Committee.[666] This is particularly the case in relation to the definitions of communications data (see paras 69–70), ICRs (paras 120–122), the removal of electronic protection (paras 263–264), and Equipment Interference (paras 292–295).

698. **The Codes of Practice will provide essential further details on how the powers in the draft Bill will be used in practice**. ***We recommend that all of them should be***

663 Written evidence from Professor John Naughton and Professor David Vincent (IPB0131)
664 Written evidence from Lord Carlile of Berriew CBE QC (IPB0017)
665 Written evidence from the UN Special Rapporteurs (IPB0102)
666 House of Commons Science and Technology Committee, *Investigatory Powers Bill: technology issues* (Third Report, Session 2015–16, HC 573)

EMBARGOED until 09:30 on 11 February 2016

published when the Bill itself is introduced to allow both Houses to conduct full scrutiny of their contents. (Recommendation 84)

Bulk data, automated analysis and the right to privacy

699. An important question raised with the Committee was how the right to privacy can be maintained when data is collected and retained in large volumes. Dr Paul Bernal explained that:

> "A key issue in relation to the gathering and retention of communications data is when the relevant rights are engaged: it is when data is gathered and retained, when it is subject to algorithmic analysis or automated filtering, or when it is subject to human examination. When looked at from what might be viewed an 'old fashioned' communications perspective, it is only when humans examine the data that 'surveillance' occurs and privacy is engaged. In relation to internet communications data this is to fundamentally miss the nature of the data and the nature of the risks. In practice, many of the most important risks occur at the gathering stage, and more at what might loosely be described as the 'automated analysis' stage."[667]

700. Christopher Graham, the Information Commissioner, told the Committee that:

> "The risks and the rights arise at the point of collection. It is a fundamental data-protection principle under the directive from which the Data Protection Act arises that information is not retained for longer than is necessary."[668]

701. Privacy International said that:

> "the Government has advanced the argument that an interference with privacy only occurs when data is examined, or "read", by a person as opposed to a machine. We disagree with this position, as ECHR case law makes clear that the interference with privacy occurs at the time of the interception regardless of whether the data is ever "read" by a person".[669]

702. This contrasts with Clause 149 (3) of the draft Bill, which says that:

> "References in this Chapter to the examination of material are references to the material being read, looked at or listened to by the persons to whom it becomes available as a result of the warrant."

703. ***We urge the Investigatory Powers Commissioner to scrutinise the automated analysis of bulk datasets conducted by the security and intelligence agencies to ensure that they are conducted appropriately and proportionately and with regard to privacy and data protection requirements. (Recommendation 85)***

EMBARGOED until 09:30 on 11 February 2016

667 Written evidence from Dr Paul Bernal (IPB0018)
668 Q 230 (Christopher Graham)
669 Written evidence from Privacy International (IPB0120)

A review provision

704. At the beginning of this report, we discussed the timescale for the Joint Committee's inquiry, within the context of the timescale for the Government's responses to various reviews and the need to legislate further before the expiry of DRIPA at the end of 2016.

705. We close our report by considering the lifespan of the Bill itself. Our witnesses pointed to a combination of the significance of the Bill, the difficulties, exposed by RIPA, of seeking adequately to "future proof" the Bill against technological change, and the shortness of the timescale available for consultation and scrutiny of its contents.

706. The case for some sort of sunset provision was summarised by the Information Commissioner:

> "The draft Bill is far reaching and has the power to affect the lives of all citizens to differing degrees. For these reasons, the bill should include a sunset clause or other provisions requiring effective post legislative scrutiny. This would ensure that measures of this magnitude remain necessary, are targeted on the right areas and are effective in practice. To fail to make this provision risks undermining public trust and confidence. It will also enable the legislation to be considered in the light of the latest jurisprudence from the CJEU and ECtHR."[670]

707. Variations on the Information Commissioner's proposal were put to us by another of other witnesses, including medConfidential,[671] Amberhawk Training Limited,[672] Dr Paul Bernal,[673] David Davis MP,[674] Privacy International,[675] and the Interception of Communications Commissioner's Office.[676] We put the suggestion to the Home Secretary when she gave evidence on 13 January. She conceded that "As technology advances, it may be necessary to revisit the powers, the legislative framework and the safeguards that are available" but argued that the Home Office's aspiration for the Bill to "stand the test of time" and provide a period of stability and certainty made any form of sunset provision undesirable. She concluded that "advances in technology are [not] going to move according to sunset clauses established by Parliament."[677]

708. **We note the reservations expressed by the Home Secretary about a sunset provision. But we are of the view that some form of review after five years would be merited. We believe that a review provision of this sort, which would require the next Parliament to revisit the powers which are in the draft Bill, would go some way to provide assurance to those who have expressed concerns over the operational case for some of these powers. The evidence of several years' operation will inform the debate. A provision which asked Parliament to revisit the intrusive powers it gives to the Executive after a period would, in our view, be a healthy way to fulfil the welcome aspirations for greater openness and legitimacy which underpin the draft Bill.**

EMBARGOED until 09:30 on 11 February 2016

670 Written evidence from the Information Commissioner (IPB0073)
671 Written evidence from medConfidential (IPB0005),
672 Written evidence from Amberhawk Training Limited (IPB0015)
673 Written evidence from Dr Paul Bernal (IPB0018)
674 Q 174 (David Davis MP)
675 Written evidence from Privacy International (IPB0120)
676 Written evidence from the Interception of Communications Commissioner's Office (IPB0101)
677 Q 259 (Theresa May MP)

709. **We agree with the Information Commissioner and others that the provisions of the Bill would benefit from detailed post-legislative scrutiny after an appropriate period. In our view, the appropriate vehicle to do this would be a specially constituted joint committee of the two Houses. This work should begin within six months of the end of the fifth year after which the Bill is enacted. Although the appointment of such a committee would be a matter for the two Houses, a provision in the Bill would provide a clear mandate and guarantee the timescale for this review.**

710. ***We recommend that a provision should be added to the face of the Bill for post-legislative scrutiny by a committee of the two Houses within six months of the end of the fifth year after the Bill is enacted. (Recommendation 86)***

EMBARGOED until 09:30 on 11 February 2016

Appendix 1: Members and interests

Members

The Rt Hon Lord Murphy of Torfaen (Chairman)
Baroness Browning
The Rt Hon Lord Butler of Brockwell
The Rt Rev Lord Bishop of Chester
Lord Hart of Chilton
The Rt Hon Lord Henley
Lord Strasburger
Victoria Atkins MP
Suella Fernandes MP
The Rt Hon David Hanson MP
Shabana Mahmood MP
Stuart C McDonald MP
Dr Andrew Murrison MP
Matt Warman MP

Declarations of interest

Victoria Atkins MP
Non-practicing barrister, in which capacity had been instructed by some of the agencies from whom the Committee was likely to hear evidence

Suella Fernandes MP
Non-practicing barrister and former Treasury Solicitor

Stuart C McDonald MP
Member of Amnesty International

Dr Andrew Murrison MP
Former serviceman and current reservist

Baroness Browning
Chair of the Advisory Committee on Business Appointments, whose remit includes providing advice to retiring heads of the intelligence and security services

Lord Hart of Chilton
Former member of Amnesty

Formerly a special adviser to two Lord Chancellors, Lord Irvine of Lairg and Lord Falconer of Thoroton

Lord Strasburger
Member of Liberty (although have not taken part in their campaigns)

Full lists of Members' interests are recorded in the Commons Register of Members' Financial Interests:

http://www.parliament.uk/business/publications/commons/

EMBARGOED until 09:30 on 11 February 2016

and the Lords Register of Interests:

http://www.parliament.uk/mps-lords-and-offices/standards-and-interests/register-of-lords-interests/

Martin Hoskins, Specialist Adviser, declared that he has been employed by, and was subsequently engaged as a consultant to, EE. He has also carried out consultancy work for Amberhawk Training Ltd. He is a member of the Open Rights Group (although has not taken part in their campaigns).

Professor Peter Sommer, Specialist Adviser, declared that in addition to his academic work, he frequently acts as an expert witness in digital evidence for both prosecution and defence interests and in civil cases. He currently holds a Home Office consultancy contract to advise on digital signature authentication of communications data.

EMBARGOED until 09:30 on 11 February 2016

Appendix 2: Call for Evidence

The following call for evidence was issued by the Committee on 30 November 2015:

The Joint Committee on the Draft Investigatory Powers Bill, chaired by Lord Murphy of Torfaen, was appointed by the two Houses of Parliament in late November 2015 to consider the Draft Investigatory Powers Bill, which was presented to the two Houses on 4 November 2015. The Committee invites any interested individuals and organisations to submit evidence to this inquiry.

The Committee in particular will explore the key issues listed below in detail, and would welcome your views on any or all of the following questions. Please note that questions are not listed here in any particular order of importance.

Written evidence should arrive no later than 21 December 2015. Public hearings will be held in November and December 2015 and January 2016. The Committee has been asked to report to the Houses, with recommendations, in February 2016. The report will receive a response from the Government. The time available for the Committee's inquiry is short, and its focus will be on the contents of the draft Bill rather than more general aspects of policy. The Committee will not consider as part of its inquiry the merits of individual cases which have been, or are now, subject to formal proceedings in courts or tribunals.

Overarching/thematic questions:

- Are the powers sought **necessary**?
  - Has the case been made, both for the new powers and for the restated and clarified existing powers?
- Are the powers sought **legal**?
  - Are the powers compatible with the Human Rights Act and the ECHR? Is the requirement that they be exercised only when necessary and proportionate fully addressed? Are they sufficiently clear and accessible on the face of the draft Bill? Is the legal framework such that CSPs (especially those based abroad) will be persuaded to comply? Are concerns around accessing journalists', legally privileged and MPs' communications sufficiently addressed?
- Are the powers sought **workable** and **carefully defined**?
  - Are the technological definitions accurate and meaningful (e.g. content vs communications data, internet connection records etc.)? Does the draft Bill adequately explain the types of activity that could be undertaken under these powers? Is the wording of the powers sustainable in the light of rapidly evolving technologies and user behaviours? Overall is the Bill future-proofed as it stands?
- Are the powers sought sufficiently **supervised**?
  - Is the authorisation process appropriate? Will the oversight bodies be able adequately to scrutinise their operation? What ability will Parliament and the public have to check and raise concerns about the use of these powers?

EMBARGOED until 09:30 on 11 February 2016

Specific questions:

General

- To what extent is it necessary for (a) the security and intelligence services and (b) law enforcement to have access to investigatory powers such as those contained in the Draft Investigatory Powers Bill?
- Are there any additional investigatory powers that security and intelligence services or law enforcement agencies should have which are not included in the draft Bill?
- Are the new offences proposed in the draft Bill necessary? Are the suggested punishments appropriate?

Interception

- Are there sufficient operational justifications for undertaking (a) targeted and (b) bulk interception?
- Are the proposed authorisation processes for such interception activities appropriate? Is the proposed process for authorising urgent warrants workable?
- Are the proposed safeguards sufficient for the secure retention of material obtained from interception?
- How well does the current process under Mutual Legal Assistance Treaties (MLATs) work for the acquisition of communications data? What will be the effect of the extra-territorial application of the provisions on communications data in the draft Bill?

Communications Data

- Are the definitions of content and communications data (including the distinction between 'entities' and 'events') sufficiently clear and practical for the purposes of accessing such data?
- Does the draft Bill allow the appropriate organisations, and people within those organisations, access to communications data?
- Are there sufficient operational justifications for accessing communications data in bulk?
- Is the authorisation process for accessing communications data appropriate?

Data Retention

- Do the proposed authorisation regime and safeguards for bulk data retention meet the requirements set out in the CJEU *Digital Rights Ireland* and the Court of Appeal *Davis* judgments?
- Is accessing Internet Connection Records essential for the purposes of IP resolution and identifying of persons of interest? Are there alternative mechanisms? Are the proposed safeguards on accessing Internet Connection Records data appropriate?

EMBARGOED until 09:30 on 11 February 2016

- Are the requirements placed on service providers necessary and feasible?

Equipment Interference

- Should the security and intelligence services have access to powers to undertake (a) targeted and (b) bulk equipment interference? Should law enforcement also have access to such powers?
- Are the authorisation processes for such equipment interference activities appropriate?
- Are the safeguards for such activities sufficient?

Bulk Personal Data

- Is the use of bulk personal datasets by the security and intelligence services appropriate? Are the safeguards sufficient for the retention and access of potentially highly sensitive data?

Oversight

- What are the advantages and disadvantages of the proposed creation of a single Judicial Commission to oversee the use of investigatory powers?
- Would the proposed Judicial Commission have sufficient powers, resources and independence to perform its role satisfactorily?
- Are the appointment and accountability arrangements for Judicial Commissioners appropriate?
- Are the new arrangements for the Investigatory Powers Tribunal including the possibility of appeal adequate or are further changes necessary?

EMBARGOED until 09:30 on 11 February 2016

Appendix 3: Delegated Powers Memorandum

Letter from the Chairman to Baroness Fookes DBE, 26 November 2015

The pre-legislative Joint Committee on the Draft Investigatory Powers Bill was appointed yesterday and had its first meeting this morning. On 4 November, the Home Office published the enclosed draft Delegated Powers Memorandum to accompany the draft Bill. The draft Memorandum offers the Home Office's view on the provisions in the draft Bill which confer powers to Ministers to make delegated legislation.

The Joint Committee considered the draft Memorandum at its first meeting and agreed that the views of the Delegated Powers and Regulatory Reform Committee would be most valuable and should be sought at the earliest opportunity. Accordingly I am writing to you to request that your Committee consider the memorandum with a view to giving the Joint Committee advice on the appropriateness of the delegations as currently drafted. We would be grateful, if possible, for a view from the Committee before the House adjourns for the Christmas recess.

The time available for our scrutiny is unusually short, and I would be most grateful if the Committee was able to offer a view before the two Houses rise for the Christmas recess.

I am copying this letter to the DPRRC clerk, Christine Salmon Percival, and to the Lords clerk of the Joint Committee on the draft Bill, Duncan Sagar.

The Home Office memorandum is available online: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473760/Delegated_Powers_Memorandum.pdf

Letter from Baroness Fookes DBE to the Chairman, 22 December 2015

The Delegated Powers and Regulatory Reform Committee welcomed the opportunity to contribute to the important work of your Joint Committee. I enclose, in response to your letter of 26 November, a submission setting out the views of the Committee on the delegations of power contained in the draft Investigatory Powers Bill. I hope that you will find it of assistance. Should an Investigatory Powers Bill be introduced into the House of Lords, we will, of course, report to the House in the usual way.

Memorandum for the Joint Committee on the Draft Investigatory Powers Bill by the Delegated Powers and Regulatory Reform Committee

1) On 26 November 2015, the Rt Hon the Lord Murphy of Torfaen, Chairman of the Joint Committee on the Draft Investigatory Powers Bill, invited the Delegated Powers and Regulatory Reform Committee to make a submission about the delegations of power in the draft Bill. The Home Office has provided a delegated powers memorandum. We welcome this opportunity to assist the Joint Committee in its work. For the most part we

EMBARGOED until 09:30 on 11 February 2016

consider the delegations of power to be unexceptionable. We would however like to draw the attention of the Joint Committee to the following matters.

Clause 43(5)(g): Power to make a direction about the publication of statistics

2) Clause 43 prohibits the disclosure of information about warrants issued under Part 2 of the Bill. Under Clause 44 it is an offence to disclose information in contravention of Clause 43. There are exceptions to the prohibition in Clause 43 and these are set out in subsection (5). One of those exceptions, in subsection (5)(g), is a disclosure made by a public postal or telecommunications operator which relates to the number of warrants in which the operator has been involved. In order to take advantage of this exception, any disclosure of information must be in accordance with a direction given by the Secretary of State. Such a direction would not be subject to any Parliamentary procedure.

3) It is clear from Clause 43(7) that a single direction may be given to more than one operator, and therefore that a direction may impose requirements which are not operator specific but which apply generally to **all** operators or **all** operators of a particular description. The Department explains in paragraph 22 of the memorandum that it is appropriate for the power to be exercisable by administrative direction because it may be necessary for it to be specific to a particular operator. **In our view, however, where the power imposes requirements which apply generally, it should not be left to a direction but contained in subordinate legislation and subject to Parliamentary scrutiny.**

Clause 55: Power to modify Clause 54 and Schedule 4

4) Part 3 of the Bill is concerned with the regime for authorising the obtaining of communications data by certain public authorities. An authorisation has to be given by a designated senior officer of an authority and has to relate to the obtaining of data for one of the public interest purposes set out in Clause 46(7). The provisions of Part 3 to a large extent reflect the existing provisions of Chapter 2 of Part 1 of the Regulation of Investigatory Powers Act 2000 ("RIPA").

5) The public authorities on whom the powers are conferred are listed in column 1 of the table in Schedule 4 to the Bill. Column 2 of the table sets out the offices, ranks or positions which a person must hold in order to be able to act as a designated senior officer. Column 3 sets out any limitations on the information which may be obtained under an authorisation given by an officer of a particular rank; and Column 4 specifies the purposes for which authorisations can be given. Clause 54 includes supplementary provision about designated senior officers.

6) Clause 55(1) confers power on the Secretary of State by regulations to amend Clause 54 and Schedule 4. The power includes a power to add or remove a public authority from the list in Schedule 4 and to modify an entry about the rank etc. of a designated senior officer. The regulations can also impose or remove restrictions on the authorisations which a particular kind of designated senior officer may give, and impose or remove restrictions on the circumstances or purposes for which authorisations may be given.

7) We accept the reasons given by the Department in paragraph 31 of the memorandum as to why there is a need for this delegated power: that is, the need to make changes to

EMBARGOED until 09:30 on 11 February 2016

reflect the creation, abolition and re-structuring of public authorities, and otherwise to reflect changes in circumstances. We also consider that, given the sensitive nature of the powers which are being given to public authorities under Part 3 of the Bill, the enhanced affirmative procedure (which is based on that in the Public Bodies Act 2011) provides an appropriate level of Parliamentary scrutiny. In contrast, section 25 of RIPA also contains powers which allow changes to be made to the relevant public authorities and to the ranks etc. of the persons who are designated for the purposes of Chapter 2 of Part 1 of that Act. In that case, however, the ordinary affirmative procedure applies where an order will have the effect of conferring the powers to obtain communications data on a new public authority. **The Committee welcomes this strengthening of scrutiny procedures under the Bill.**

8) Clause 56(1) sets out circumstances in which the negative rather than the enhanced affirmative procedure will apply to regulations under Clause 55(1). These are where the regulations only have effect:

- to remove a public authority from the list in Column 1 of the table in Schedule 4 and make consequential modifications; or
- to modify the list of ranks, offices etc. that must be held by a designated senior officer as set out in Column 2 of that table.

9) We consider the negative procedure is appropriate where the regulations remove a public authority from the list in Column 1 of the table in Schedule 4, since their sole effect will be to reduce the number of bodies who are capable of exercising the powers to obtain communications data. We are not however convinced that the negative procedure affords the appropriate level of scrutiny in all cases where it is proposed to modify Column 2 of the table in Schedule 4. We consider the requirement for an authorisation to be given at a high level within an organisation offers an important protection against an inappropriate use of the powers conferred by Part 3. **Accordingly, we think that any regulations modifying Column 2 which have the effect of lowering the level at which an authorisation has to be given should be subject to at least the affirmative procedure.**

Clause 57: Power to amend the definition of a designated senior officer in a local authority

10) Clause 57 provides for a local authority to be a "relevant public authority" for the purposes of Part 3 Subsection (2) of that clause defines who is a designated senior officer in a local authority, and subsection (4) confers a power on the Secretary of State by regulations to amend subsection (2). Regulations under Clause 57(4) are subject to the negative procedure. **For the reasons given in paragraph 9, we consider that any regulations which have the effect of lowering the level at which an authorisation has to be given should be subject to at least the affirmative procedure.**

Clause 177: Power to modify the functions of the Investigatory Powers Commissioner and other Judicial Commissioners

11) Clause 177(1) confers a power on the Secretary of State by regulations to modify the functions of the Investigatory Powers Commissioner (IPC) and other Judicial Commissioners. By virtue of subsection (2) of that clause, this power includes a power

EMBARGOED until 09:30 on 11 February 2016

to amend legislation, including a power to amend the provisions of the Bill itself once enacted.

12) In paragraph 68 of the memorandum, the Department explains the need for this power as enabling it "to respond quickly and flexibly" to changes in the statutory functions of public authorities, or changes in the circumstances affecting such functions, to ensure that the IPC and the other Judicial Commissioners have the appropriate powers to carry out their oversight functions. The memorandum also explains that the power would allow further detail to be added to the functions of the IPC and the other Judicial Commissioners.

13) While this explanation may indicate that some form of power is needed to allow modifications to be made to the functions of the IPC and the other Judicial Commissioners, we are concerned about the very wide scope of the power conferred by Clause 177, particularly as it would allow amendments to be made to provisions of the Bill itself. Parts 2, 5 and 6 of the Bill require the approval of the IPC or another Judicial Commissioner for warrants issued under any of those Parts. On the face of it, Clause 177 would enable the Secretary of State by regulations to make amendments to these functions so as to weaken the approval regime, and even to provide for their removal in specific cases. The Government have made it clear in the guidance covering the draft Bill that the role of the IPC and the other Judicial Commissioners in approving warrants provides a crucial safeguard over the interception etc. powers conferred by the Bill.

14) **In the circumstances, it seems to us inappropriate for the powers conferred by Clause 177 to be drawn in a way that would allow the Judicial Commissioners' functions in respect of the approval of warrants to be modified by subordinate legislation.**

Clause 201(2): Power to make consequential provision

15) Clause 201(2) confers a power on the Secretary of State by regulations to make such consequential provision as he or she considers appropriate. In common with many provisions of this kind, Clause 201(3) provides that this power may be exercised by amending or otherwise modifying provisions of primary or subordinate legislation.

16) Clause 201(3) refers to "enactments" and it is clear from the way in which this expression is defined in Clause 195(1) that the powers conferred by Clause 201(3) include the power to amend or otherwise modify **future** enactments. While it is reasonable for there to be a need to amend past enactments to ensure that they fit with the provisions of the Bill, the same does not necessarily apply to future legislation which should be capable of taking account of the Bill's provisions when it is enacted. Accordingly, we would ordinarily expect a convincing case to be made in the memorandum for a power to use subordinate legislation to amend future primary legislation. In this case, the memorandum says nothing about why it is necessary to have the power to amend future enactments. Two precedents are given in paragraph 113 of the memorandum, but in neither case does the power include a power to amend future enactments. **We regard this aspect of the power as being inappropriate in the absence of a reasonable explanation for why it is needed.**

17) Regulations under Clause 201(2) are subject to the affirmative procedure where they amend or repeal a provision of primary legislation. The negative procedure applies in all other cases, including where the regulations **otherwise modify** a provision of primary

EMBARGOED until 09:30 on 11 February 2016

legislation. Non-textual modification of primary legislation can however be used to make changes which are no less significant than textual amendments. **We have expressed the view, therefore, on a number of occasions–most recently in our reports on the Scotland Bill[678] and the Enterprise Bill[679]–that, as a matter of general principle, non-textual modifications of primary legislation should be subject to the same level of Parliamentary scrutiny as textual amendments, namely, the affirmative procedure.**

EMBARGOED until 09:30 on 11 February 2016

678 Delegated Powers and Regulatory Reform Committee, *Scotland Bill; Trade Union Bill; Enterprise Bill; Draft Legislative Reform (Exempt Lotteries) Order 2016* (15th Report, Session 2015–16, HL Paper 64) paras 10 to 13

679 Delegated Powers and Regulatory Reform Committee, *Enterprise Bill [HL]: European Union Referendum Bill* (9th Report, Session 2015–16, HL Paper 42) paras 17 to 21

Appendix 4: Human Rights Memorandum

Letter from the Chairman to the Rt Hon Harriet Harman QC MP, 26 November 2015

The pre-legislative Joint Committee on the Draft Investigatory Powers Bill was appointed yesterday and had its first meeting this morning. On 4 November, the Home Office published the enclosed draft Human Rights Memorandum to accompany the draft Bill. The draft Memorandum offers the Home Office's view on the provisions in the draft Bill which it considers engage human rights considerations.

The Joint Committee considered the draft Memorandum at its first meeting and, in view of the importance of the human rights dimension to this inquiry, agreed that the views of the Joint Committee on Human Rights would be most valuable and should be sought at the earliest possible opportunity. Accordingly I am writing to you to request that your Committee consider the memorandum with a view to giving the Joint Committee advice on the provisions covered in the memorandum as well as to make any other comments which your Committee feels are relevant to our scrutiny of the draft Bill.

The time available for our scrutiny is unusually short, and I would be most grateful if the Committee was able to offer a view before the two Houses rise for the Christmas recess.

I am copying this letter to the JCHR clerk, Robin James, and to the Lords clerk of the Joint Committee on the draft Bill, Duncan Sagar.

The Home Office memorandum is available online: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473763/European_Convention_on_Human_Rights_Memorandum.pdf

Letter to the Chairman from the Rt Hon Harriet Harman QC MP, 25 January 2016

Thank you for your letter of 26 November asking my Committee to consider the draft Human Rights Memorandum accompanying the Draft Investigatory Powers Bill with a view to advising your Committee on the provisions covered in the Memorandum plus any other comments my Committee might have about the Bill.

As you may be aware, the Joint Committee on Human Rights was one of the last committees to be established following the General Election and since it was constituted at the end of October it has had a very full programme of work. The Committee and its staff have been fully occupied with its other priorities, including its inquiry into the Government's policy on the use of drones for targeted killing. As my Committee's staff made clear to your Committee's staff at the beginning of December, it has therefore not proved possible to consider the human rights implications of the draft Investigatory Powers Bill in time to be of assistance to your Committee in its consideration of the Bill.

My Committee will of course scrutinise the Bill itself for human rights compatibility when it is published.

EMBARGOED until 09:30 on 11 February 2016

Appendix 5: List of abbreviations

ATCSA 2001	Anti-Terrorism Crime and Security Act 2001
BCS	British Computer Society
BPDs	Bulk Personal Datasets
CD	Communications Data
CDI	Content-Derived Information
CDNs	Content Delivery Networks
CDRs	Call Data Records
CJEU	Court of Justice of the European Union
CSPs	Communications Service Providers
CTSA 2015	Counter Terrorism and Security Act 2015
DRIPA 2014	Data Retention and Investigatory Powers Act 2014
DPI:	Deep Packet Inspection
DPRRC	Delegated Powers and Regulatory Reform Committee
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EI	Equipment Interference
GCHQ	Government Communications Headquarters
GPS	Global Positioning System
HRA 1998	Human Rights Act 1998
HMRC	Her Majesty's Revenue and Customs
ICCPR	International Covenant on Civil and Political Rights
ICO	The Information Commissioner's Office
ICRs	Internet Connection Records
IMSI	International Mobile Subscriber Identity
IOCCO	The Interception of Communications Commissioner's Office
IP address	Internet Protocol address
IPC	The Investigatory Powers Commissioner
IPT	The Investigatory Powers Tribunal
ISC	The Intelligence and Security Committee of Parliament
ISCom	The Intelligence Services Commissioner
ISP	Internet Service Provider
ISPA	The Internet Service Providers' Association
JCs	Judicial Commissioners
LPP	Legal Professional Privilege
MI5	The Security Service

EMBARGOED until 09.30 on 11 February 2016

MLAT	Mutual Legal Assistance Treaty
NAFN	The National Anti-Fraud Network
OSC	The Office of Surveillance Commissioners
OTT	Over The Top Providers
PACE	Police and Criminal Evidence Act 1984
RCD	Related Communications Data
RIM	Research in Motion
RIPA	Regulation of Investigatory Powers Act 2000
RUSI	The Royal United Services Institute
SFO	The Serious Fraud Office
SIS:	The Secret Intelligence Service
SPoC	Single Point of Contact
Tor	The Onion Router
URL	Uniform Resource Locator
VPN	Virtual Private Networks

EMBARGOED until 09:30 on 11 February 2016

Formal Minutes

Wednesday 3 February 2016

Members present:

Lord Murphy of Torfaen, in the Chair

Baroness Browning	Victoria Atkins
Lord Butler of Brockwell	Suella Fernandes
The Bishop of Chester	Rt Hon David Hanson
Lord Hart of Chilton	Stuart C McDonald
Lord Henley	Shabana Mahmood
Lord Strasburger	Dr Andrew Murrison
	Matt Warman

Draft Report (*Draft Investigatory Powers Bill*), proposed by the Chairman, brought up and read.

Ordered, That the draft Report be read a second time, paragraph by paragraph.

Paragraphs 1 to 322 read and agreed to.

Paragraph 323 read, as follows:

We recognise that, given the global nature of the internet, the limitation of the bulk powers to "overseas-related" communications may make little difference in practice to the data that could be gathered under these powers. We recommend that the Government should explain the value of including this language in the Bill.

Amendment proposed, at the end to add "and consult on alternative ways of excluding people in the UK from the scope of bulk interception and bulk equipment interference warrants".—*(Stuart C. McDonald.)*

Question put, That the Amendment be made.

The Committee divides.

Contents, 4	Not-Contents, 10
Stuart C. McDonald	Victoria Atkins
Shabana Mahmood	Baroness Browning
Lord Murphy of Torfaen	Lord Butler of Brockwell
Lord Strasburger	The Bishop of Chester
	Suella Fernandes
	Mr David Hanson
	Lord Hart of Chilton
	Lord Henley
	Dr Andrew Murrison
	Matt Warman

Question accordingly negatived.

Paragraph agreed to.

EMBARGOED until 09:00 on 11 February 2016

Paragraphs 324 to 432 read and agreed to.

Paragraph 433 read.

Amendment proposed, to leave out the paragraph and insert—

"In order to provide a full 'double-lock' where judges can decide on the merits of each case, the Committee recommends the deletion of clauses 19(2), 90(2), 109(2), 123(2), 138(2), 155(2)." —*(Stuart C. McDonald.)*

Question put, That the Amendment be made.

The Committee divides.

Contents, 4	Not-Contents, 10
Stuart C. McDonald	Victoria Atkins
Shabana Mahmood	Baroness Browning
Dr Andrew Murrison	Lord Butler of Brockwell
Lord Strasburger	The Bishop of Chester
	Suella Fernandes
	Mr David Hanson
	Lord Hart of Chilton
	Lord Henley
	Lord Murphy of Torfaen
	Dr Andrew Murrison
	Matt Warman

Amendment proposed, to leave out the paragraph and insert—

"In order to clarify the meaning of judicial review in the context of this Bill, the Committee recommends the addition of some further clauses on the face of the Bill detailing the exact remit of the Judicial Commissioner when making their decision about authorisation of these warrants. These should specify that the Judicial Commissioner must take into account necessity and proportionality when making the decision, and consider the merits of the case on the basis of the written evidence submitted to the Secretary of State." —*(Lord Strasburger.)*

Question put, That the Amendment be made.

The Committee divides.

Contents, 6	Not-Contents, 7
The Bishop of Chester	Victoria Atkins
Mr David Hanson	Baroness Browning
Shabana Mahmood	Lord Butler of Brockwell
Lord Murphy of Torfaen	Suella Fernandes
Dr Andrew Murrison	Lord Hart of Chilton
Lord Strasburger	Lord Henley
	Matt Warman

Question accordingly negatived.

Paragraph agreed to.

EMBARGOED until 09:30 on 11 February 2016

Paragraphs 434 to 481 read and agreed to.

Paragraph 482 read.

Amendment proposed, to leave out the paragraph and insert—

"The Committee recommends that the Government considers whether, given the lower level of authorisation already applied to communications data, it is necessary to have these emergency procedures in place." — *(Victoria Atkins.)*

Question put, That the Amendment be made.

The Committee divides.

Contents, 5	Not-Contents, 9
Victoria Atkins	Lord Butler of Brockwell
Baroness Browning	The Bishop of Chester
Suella Fernandes	Lord Hart of Chilton
Lord Henley	Lord Henley
Matt Warman	Mr David Hanson
	Shabana Mahmood
	Lord Murphy of Torfaen
	Dr Andrew Murrison
	Lord Strasburger

Question accordingly negatived.

Paragraph agreed to.

Paragraphs 483 to 496 read and agreed to.

Paragraph 497 read.

Question put, That the paragraph stand part of the Report.

The Committee divides.

Contents, 7	Not-Contents, 7
Lord Butler of Brockwell	Victoria Atkins
Mr David Hanson	Baroness Browning
Stuart C. McDonald	The Bishop of Chester
Shabana Mahmood	Suella Fernandes
Lord Murphy of Torfaen	Lord Hart of Chilton
Dr Andrew Murrison	Lord Henley
Lord Strasburger	Matt Warman

There being no majority for removing the paragraph, it was agreed to.

Paragraphs 498 to 501 read and agreed to.

Paragraph 502 read.

Amendment proposed, to leave out the paragraph and insert—

EMBARGOED until 09:30 on 11 February 2016

"The Committee is unconvinced by the Government's argument that National Security and Technical Capability notices are "of a different order" to other warrants and recommends that they are also subject the 'double-lock' authorisation procedure." —*(Stuart C. McDonald.)*

Question put, That the Amendment be made.

The Committee divides.

Contents, 2	Not-Contents, 12
Stuart C. McDonald	Victoria Atkins
Lord Strasburger	Baroness Browning
	Lord Butler of Brockwell
	The Bishop of Chester
	Suella Fernandes
	Mr David Hanson
	Lord Hart of Chilton
	Lord Henley
	Shabana Mahmood
	Lord Murphy of Torfaen
	Dr Andrew Murrison
	Matt Warman

Question accordingly negatived

Paragraph agreed to.

Paragraphs 503 to 563 read and agreed to.

Paragraph 564 read.

Amendment proposed, to leave out the paragraph and insert—

"The Committee has concerns as to the level of protection which the Bill affords to the communications of Parliamentarians. The Bill affords a measure of protection to communications between an MP and his constituents but the precise nature of this protection and the protection afforded to other communications which a Parliamentarian may have is not clear. This may include, for example, communications with a whistleblower (which might be regarded as part of a Parliamentarian's remit) or investigative journalist (which might be regarded as conducive to a healthy democracy).

The protections afforded by clause 16 relate solely to targeted interception and examination warrants. These protections should be applicable in the case of all warrants and the acquisition of communications data. Further, the protections afforded by the code of practice to be made under Schedule 6 relate only to communications data arising in respect of communications betweens and their constituents. The protections should be extended to cover all categories of warrants and all communications between an MP and a third party arising as a result of his position as an MP."—*(Stuart C. McDonald.)*

Question put, That the Amendment be made.

The Committee divides.

EMBARGOED until 09:30 on 11 February 2016

Contents, 6	Not-Contents, 8
Lord Butler of Brockwell	Victoria Atkins
The Bishop of Chester	Baroness Browning
Stuart C. McDonald	Suella Fernandes
Shabana Mahmood	Mr David Hanson
Lord Murphy of Torfaen	Lord Hart of Chilton
Lord Strasburger	Lord Henley
	Dr Andrew Murrison
	Matt Warman

Question accordingly negatived.

Paragraph agreed to.

Paragraphs 565 to 587 read and agreed to.

Paragraph 588 read, as follows:

We recommend the Lord Chief Justice should have the power to appoint Judicial Commissioners following consultation with his judicial opposite numbers in Scotland and Northern Ireland and with the Prime Minister, Scottish Ministers and he First Minister and deputy First Minister in Northern Ireland. This will ensure public confidence that the Judicial Commissioners are independent and impartial and enhance political confidence in the Judicial Commissioners. The Lord Chief Justice will also be able to assess the impact of appointments on the work of the High Court and the Court of Appeal which must not be impaired by the creation of the Judicial Commissioners. The Judicial Appointments Commission must also be consulted to ensure the appointments procedure is fair and transparent.

Amendment proposed, in line 1, to leave out from beginning to "The" in line 7 and insert—

"We recommend the Prime Minister should be able to exercise the power to appoint Judicial Commissioners only following consultation with the Lord Chief Justice. This will ensure Judicial Commissioners have the confidence of the political establishment. The impact of the creation of the Judicial Commissioners on the work of the High Court and Court of Appeal will be taken into account through consultation with the Lord Chief Justice."—*(Baroness Browning.)*

Question put, That the Amendment be made.

The Committee divides.

Contents, 5	Not-Contents, 9
Victoria Atkins	Lord Butler of Brockwell
Baroness Browning	The Bishop of Chester
Suella Fernandes	Mr David Hanson
Lord Henley	Lord Hart of Chilton
Matt Warman	Stuart C. McDonald
	Shabana Mahmood
	Lord Murphy of Torfaen
	Dr Andrew Murrison
	Lord Strasburger

Question accordingly negatived.

EMBARGOED until 09:30 on 11 February 2016

Paragraph agreed to.

Paragraphs 589 to 607 read and agreed to.

Paragraph 608 read.

Amendment proposed, to leave out the paragraph and insert—

"Clause 177 gives the Home Secretary an unfettered power to modify the functions of the Judicial Commissioners. This is inappropriate if the Judicial Commissioners are to be seen as independent of Government. It is unclear why the power is required. Changes to the Judicial Commissioners' functions should be confined to primary legislation, as a matter of this importance should be subject to full debate by both Houses of Parliament. We recommend the power be removed from the Bill."—*(Stuart C. McDonald.)*

Question put, That the Amendment be made.

The Committee divides.

Contents, 5	Not-Contents, 9
Stuart C. McDonald	Victoria Atkins
Shabana Mahmood	Baroness Browning
Lord Murphy of Torfaen	Lord Butler of Brockwell
Dr Andrew Murrison	The Bishop of Chester
Lord Strasburger	Suella Fernandes
	Mr David Hanson
	Lord Hart of Chilton
	Lord Henley
	Matt Warman

Question accordingly negatived.

Paragraph agreed to.

Paragraphs 609 to 710 read and agreed to.

Summary agreed to.

Appendices to the Report agreed to.

Resolved, That the Report be the Report of the Committee to both Houses.

Ordered, That the Report is made to the House of Lords and that Mr David Hanson make the Report to the House of Commons.

Written evidence was ordered to be reported.

Ordered, That embargoed copies of the Report be made available, in accordance with the provisions of Standing Order No. 134 of the House of Commons.

The Committee adjourned *sine die.*

EMBARGOED until 09:30 on 11 February 2016

Witnesses

The following witnesses gave evidence. Transcripts can be viewed on the Committee's inquiry page at http://www.parliament.uk/draft-investigatory-powers.

Monday 30 November 2015

	Question number
Richard Alcock and **Paul Lincoln**, Home Office, and **Lewis Neal**, Foreign and Commonwealth Office	Q 1–25
Richard Berry, National Police Chiefs' Council, **Keith Bristow** and **Chris Farrimond**, National Crime Agency, and **Simon York**, HMRC	Q 26–38

Wednesday 2 December 2015

The Rt Hon Sir Mark Waller, Intelligence Services Commissioner	Q 39–46
The Rt Hon Sir Stanley Burnton, Interception of Communications Commissioner, **Jo Cavan**, Interception of Communications Commissioner's Office, **The Rt Hon Lord Judge**, Chief Surveillance Commissioner, and **Clare Ringshaw-Dowle**, Chief Surveillance Inspector	Q 47–60
David Anderson QC, Independent Reviewer of Terrorism Legislation, and **Professor Michael Clarke**, Royal United Services Institute	Q 61–75

Monday 7 December 2015

Professor Ross Anderson, University of Cambridge, **Dr Paul Bernal**, University of East Anglia, **Professor Sir David Omand GCB**, King's College London, and **Professor Mark Ryan**, University of Birmingham	Q 76–93
The Rt Hon Lord Blunkett and **The Rt Hon Owen Paterson MP**	Q 94–100

Wednesday 9 December 2015

Mark Hughes, BT Security, **Adam Kinsley**, Sky, and **Hugh Woolford**, Virgin Media	Q 101–115
James Blessing, Internet Service Providers' Association (ISPA), Keycom, and **Adrian Kennard**, Andrews & Arnold Ltd	Q 116–126
Shami Chakrabati, Liberty, **Jim Killock**, Open Rights Group, **Renate Samson**, Big Brother Watch, and **Caroline Wilson Palow**, Privacy International	Q 127–136

Monday 14 December 2015

Tim Musson, The Law Society of Scotland, **Colin Passmore**, The Law Society, **Bob Satchwell**, Society of Editors, and **Andy Smith**, National Union of Journalists	Q 137–144
Adrian Gorham, O2 Telefónica, **Jonathan Grayling**, EE, **Mark Hughes**, Vodafone, and **Simon Miller**, 3	Q 145–161

EMBARGOED until 09:30 on 11 February 2016

Wednesday 16 December 2015

Michael Atkinson, National Policing Data Communications Group, **Detective Superintendent Paul Hudson**, Metropolitan Police Service, and **Detective Superintendent Matt Long**, National Crime Agency	Q 162–173
The Rt Hon David Davis MP and **Baroness Jones of Moulescoomb**	Q 174–185
Peter Carter QC, **Martin Chamberlain QC**, **Matthew Ryder QC**, and **Graham Smith**, Bird & Bird LLP	Q 186–196

Monday 21 December 2015

Rachel Griffin, Suzy Lamplugh Trust, **Rachel Logan**, Amnesty International UK, and **Alan Wardle**, National Society for the Prevention of Cruelty to Children	Q 197–206
Professor Bill Buchanan, Edinburgh Napier University, **Eric King**, and **Erka Koivunen**, F-Secure Corporation	Q 207–215
Professor Christopher Forsyth, Policy Exchange, and **Robin Simcox**, Henry Jackson Society	Q 216–223

Wednesday 6 January 2016

Christopher Graham, Information Commissioner	Q 224–233
William E. Binney, retired Technical Director of the United States National Security Agency, and **Jesper Lund**, The Danish IT Political Association	Q 234–249
Sir J. Bruce Robertson, New Zealand Commissioner of Security Warrants	Q 250–258

Wednesday 13 January 2016

The Rt Hon Theresa May MP, Home Secretary	Q 259–282

EMBARGOED until 09:30 on 11 February 2016

Published written evidence

The following written evidence was received and can be viewed on the Committee's inquiry web page at www.parliament.uk/draft-investigatory-powers. IPB numbers are generated by the evidence processing system and so may not be complete.

1 Access Now (IPB0112)
2 Access Now et al. (IPB0109)
3 ADS (IPB0083)
4 Amberhawk Training Limited (IPB0015)
5 Amnesty International UK (IPB0074)
6 David Anderson Q.C (IPB0152)
7 Andrews & Arnold Ltd (IPB0001)
8 Andrews & Arnold Ltd (IPB0028)
9 Apple Inc. and Apple Distribution International (IPB0093)
10 ARTICLE 19 (IPB0052)
11 Bar Council (IPB0134)
12 Ian Batten (IPB0090)
13 BCS, The Chartered Institute for IT (IPB0075)
14 Dr Paul Bernal (IPB0018)
15 Anam Bevardis (IPB0100)
16 Krishan Bhasin (IPB0034)
17 Big Brother Watch (IPB0007)
18 Paul Biggs (IPB0084)
19 Bingham Centre for the Rule of Law (IPB0055)
20 William Binney (IPB0009)
21 William Binney (IPB0161)
22 Brass Horn Communications (IPB0067)
23 BT (IPB0151)
24 Kevin Cahill (IPB0145)
25 Kevin Cahill (IPB0162)
26 Duncan Campbell (IPB0069)
27 Duncan Campbell (IPB0124)
28 Lord Carlile of Berriew CBE QC (IPB0017)
29 Center for Democracy & Technology (IPB0110)
30 Martin Chamberlain QC (IPB0133)
31 Chartered Institute of Legal Executives (IPB0041)
32 Chartered Institute of Library and Information Professionals (CILIP) (IPB0104)
33 Tom Chiverton (IPB0023)
34 Howard Clark (IPB0070)
35 Dr Richard Clayton (IPB0085)
36 Naomi Colvin (IPB0063)
37 Committee on the Administration of Justice ('CAJ') (IPB0025)
38 Ray Corrigan (IPB0053)

EMBARGOED until 09:30 on 11 February 2016

39 COSLA (IPB0042)
40 Mr Simon Cramp (IPB0024)
41 Criminal Cases Review Commission (IPB0031)
42 Crown Prosecution Service (IPB0081)
43 Cryptomathic Ltd (IPB0115)
44 Simon Davies (IPB0121)
45 Dr Andrew Defty (IPB0050)
46 Digital–Trust CIC (IPB0117)
47 Jamie Dowling (IPB0149)
48 Mark Dziecielewski (IPB0082)
49 EE (IPB0139)
50 Electronic Frontier Foundation (IPB0119)
51 Entanet International Limited (IPB0022)
52 Equality and Human Rights Commission (IPB0136)
53 Eris Industries Limited (IPB0011)
54 Facebook Inc., Google Inc., Microsoft Corp., Twitter Inc., and Yahoo Inc. (IPB0116)
55 F-Secure Corporation (IPB0118)
56 Mr Peter Gill (IPB0008)
57 Professor Anthony Glees (IPB0150)
58 Global Network Initiative (GNI) (IPB0080)
59 GreenNet Limited (IPB0132)
60 Wendy M. Grossman (IPB0068)
61 Guardian News & Media (IPB0040)
62 Cheryl Gwyn, Inspector-General of Intelligence and Security (IPB0158)
63 Dr Christian Heitsch (IPB0111)
64 Dr Tom Hickman (IPB0039)
65 Home Office (IPB0159)
66 Home Office (IPB0147)
67 Home Office (IPB0146)
68 Human Rights Watch (IPB0123)
69 Dr Julian Huppert (IPB0130)
70 ICAEW (IPB0044)
71 The Information Commissioner's Office (IPB0073)
72 The Institute for Human Rights and Business (IHRB) (IPB0094)
73 Interception of Communications Commissioner's Office (IPB0101)
74 Internet Service Providers' Association (ISPA) (IPB0137)
75 Internet Service Providers' Association (ISPA) (IPB0164)
76 IT-Political Association of Denmark (IPB0103)
77 Jisc (IPB0019)
78 The Rt Hon Lord Judge (IPB0020)
79 Justice (IPB0148)
80 Mr. Bernard Keenan, Dr. Orla Lynskey and Professor Andrew Murray (IPB0071)

EMBARGOED until 09:30 on 11 February 2016

81 Eric King (IPB0106)
82 Mr Gareth Kitchen (IPB0059)
83 Martin Kleppmann (IPB0054)
84 National Police Chiefs Council, HM Revenue and Customs and the National Crime Agency (IPB0140)
85 The Law Society of England and Wales (IPB0105)
86 The Law Society of Scotland (IPB0128)
87 Liberty (IPB0143)
88 LINX (IPB0097)
89 Christopher Lloyd (IPB0056)
90 Local Government Association (LGA), National Anti-Fraud Network (NAFN), Chartered Trading Standards Institute and Association of Chief Trading Standards Officers (IPB0051)
91 Annie Machon (IPB0064)
92 The Rt Hon Theresa May MP (IPB0165)
93 Mr Ray McClure (IPB0016)
94 McEvedys Solicitors & Attorneys Ltd (IPB0138)
95 medConfidential (IPB0005)
96 Media Lawyers Association (IPB0010)
97 Mental Welfare Commission for Scotland (IPB0029)
98 Dr. Glyn Moody (IPB0057)
99 Ms Susan Morgan (IPB0043)
100 Mozilla (IPB0099)
101 Cian C. Murphy and Natasha Simonsen (IPB0096)
102 Muslim Council of Britain (IPB0095)
103 National Union of Journalists (NUJ (IPB0078)
104 Professor John Naughton and Professor David Vincent (IPB0131)
105 Network for Police Monitoring (Netpol) (IPB0087)
106 New America's Open Technology Institute (IPB0086)
107 News Media Association (IPB0012)
108 NSPCC (IPB0049)
109 The Odysseus Trust (IPB0030)
110 Ofcom (IPB0129)
111 Open Intelligence (IPB0066)
112 Open Rights Group (IPB0108)
113 William Perrin (IPB0156)
114 Simon Pooley (IPB0060)
115 Privacy International (IPB0120)
116 Public Concern at Work (IPB0077)
117 Zara Rahman (IPB0079)
118 The Hon Sir Bruce Robertson (IPB0141)
119 Ms. Coleen Rowley (IPB0058)
120 Peter Rush (IPB0033)

EMBARGOED until 09:30 on 11 February 2016

121 Matthew Ryder QC (IPB0142)
122 Scottish PEN (IPB0076)
123 Serious Fraud Office (IPB0153)
124 Graham Smith (IPB0126)
125 Graham Smith (IPB0157)
126 Winston Smith (IPB0062)
127 Dr. Christopher Soghoian (IPB0167)
128 Giuseppe Sollazzo (IPB0032)
129 TalkTalk (IPB0154)
130 techUK (IPB0088)
131 Alice Thompson (IPB0072)
132 HH Judge Peter Thornton QC (IPB0026)
133 The Tor Project (IPB0122)
134 Trading Standards North West, Intellectual Property Group (IPB0092)
135 UN Special Rapporteurs (IPB0102)
136 Virgin Media (IPB0160)
137 Philip Virgo (IPB0061)
138 Vodafone (IPB0127)
139 William Waites (IPB0089)
140 The Rt Hon Sir Mark Waller (IPB0021)
141 Daniel Walrond (IPB0065)
142 Rev Cecil Ward (IPB0013)
143 David Wells (IPB0166)
144 Peter White (IPB0004)
145 Adrian Wilkins (IPB0003)
146 Professor Andrew Woods (IPB0114)
147 Professor Lorna Woods (IPB0163)
148 Yahoo (IPB0155)

EMBARGOED until 09:30 on 11 February 2016